MeerCAT®-Pro

User Manual

Applied Visions, Inc (AVI), Secure Decisions Division, 6 Bayview Avenue, Northport, NY 11768
www.SecureDecisions.AVI.com, (631) 754-4920, meercat@securedecisions.com

MeerCAT®-Pro

Version 3.2 Release

© Copyright 2007-2011. All rights reserved. Applied Visions, Inc.
Distribution of this work is prohibited unless prior written permission is obtained from the copyright holder.

MeerCAT is a trademark of Applied Visions, Inc.
All other trademarks and copyright are the property of their respective owners.

TABLE OF CONTENTS

1 Introducing MeerCAT 6
1.1 What is MeerCAT? 6
1.2 What are the Benefits of MeerCAT? 6
1.3 What are MeerCAT's Key Features & Functions? 7
2 Getting Help With MeerCAT 9
2.1 MeerCAT Technical Support 9
2.2 MeerCAT Feedback and Additional Information 9
2.3 Licensing 9
3 Accessing and Navigating MeerCAT 10
3.1 Controlling MeerCAT 10
Coordinated Views 10
Context Menus 10
3.2 Customizing the MeerCAT Console 11
Views 11
Preferences 14
4 Importing Data Into MeerCAT 15
4.1 Importing Kismet Data 15
4.2 Importing NetStumbler Data 16
4.3 Bulk Import Kismet Data 17
4.4 Known Devices 18
Manually Adding Known Devices 19
Importing Known Devices from a CSV File 20
4.5 Importing Wired Capture Data 20
5 Using MeerCAT – Fundamental Tools 21
5.1 MeerCAT Console 21
5.2 Device Explorer View 21
Toolbar 23
Illustrative Windows 24
5.3 Networks View 27
Toolbar 28
5.4 Clients View 28
Toolbar 28
5.5 3D Geographic View 28
Controls 30
Toolbar 31
3D Specialized Controls 32
5.6 Network Topology View 33
Toolbar 35
5.7 Navigator View 35
Selection / Highlighting 36
Panning 36
Zooming 36

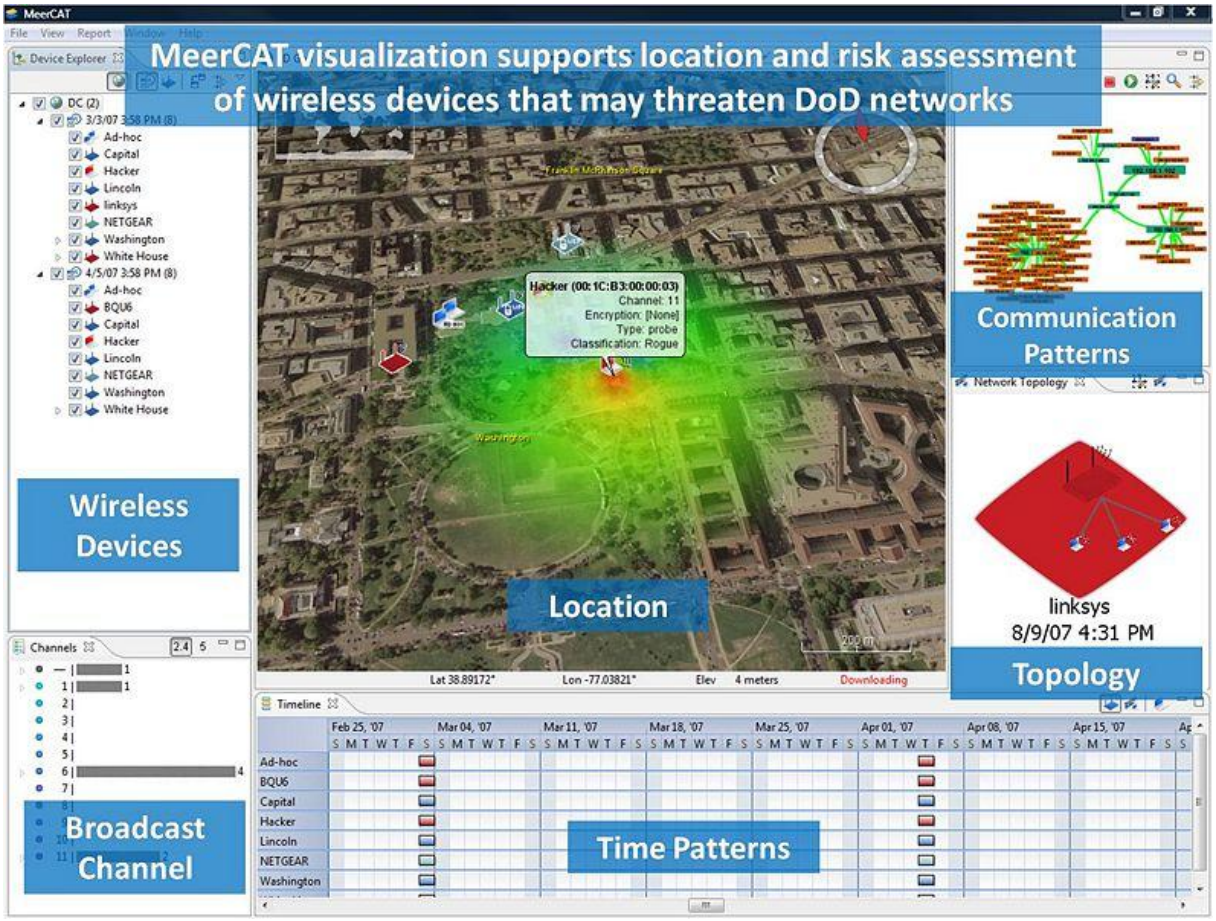
Searching 36
Toolbar 37
5.8 Channels View 40
5.9 Timeline View 41
Toolbar 42
5.10 Device History View 44
Toolbar 45
5.11 Overlays Details 45
Toolbar 45
5.12 Legend View 46
5.13 Image Viewer 48
Adding Images 48
Displaying Images 49
Removing Images 49
User Controls 49
Toolbar 49
5.14 Mission Mapping 50
Preferences Page for Mission Mapping 50
Choosing a Color for the Mission 51
Assigning the Mission to an Access Point 51
Color the Network by Mission 52
Colored by Mission 53
Group by Mission 54
6 Communication Flow Graph 55
6.1 Flows View 55
Graph Type 56
Nodes 56
Links 58
Filter 58
User-Graph Interaction 58
Toolbar 59
Communication Patterns Usage Scenario 59
WiFi LAN Example 63
WiFi Broadcast Domain Example 66
6.2 Flow Details 68
Toolbar 68
6.3 Wired Captures 69
Wired Captures View 69
Flows View 69
Flow Details View 70
7 Reporting 71
7.1 Reporting Features 71
Generate Report 71
Copy Screenshot of Active View 72

Save Screenshot of Active View 72
Email Screenshot of Active View 72
Drag and Drop 72
View Annotations 72
7.2 Report Templates 73
Images 74
Tables 74
Annotations 74
8 Other Preference Options 74
8.1 Bookmarks 74
8.2 Flow Colors 76
8.3 General Colors 79
8.4 Import Folder 80
8.5 Maintain Perspectives 81
8.6 Reporting Options 81
8.7 Tags 82
9 Frequently Asked Questions 85

1 Introducing MeerCAT

1.1 What is MeerCAT?

MeerCAT (Mobile Cyber Asset Tracks) is a visualization tool specifically developed to help users locate wireless assets and networks, and assess the risks to their organization. It is designed for post-hoc analysis of data acquired from site surveys or wireless security audits such as 'war drives' that discover, identify and locate wireless transmitters.



1.2 What are the Benefits of MeerCAT?

Organizations are deploying or being exposed to wireless local area networks (LANs) to support mobile connectivity. However, wireless LANs present unique security challenges, as it is easy to introduce unauthorized or intercept authorized wireless signals in organizational networks. While there are numerous systems designed to help locate and assess wireless activity, they generate significant data that require experience and expertise to correlate and interpret. One of the challenges is to quickly turn the wealth of

data into meaningful and actionable information. Visualization is an effective way to make sense of this data.

MeerCAT arms users with advanced **visual analytics** specifically **designed to facilitate and expedite the analysis of wireless discovery data** to quickly locate and assess the risks of wireless assets. Professionals can use MeerCAT to locate both authorized and unauthorized (rogue) access points and unsecured wireless devices. MeerCAT users can also 'see' with what assets are wireless devices connecting to.

Among the benefits of using MeerCAT to analyze wireless risks:

- **Supports post-hoc analysis of multiple wireless discovery sessions** for periodic security audits and on-going assessment of external and internal wireless networks.
- Provides interactive and coordinated geospatial, topological and spatio-temporal views to **quickly locate potential security issues**, and efficiently identify relevant vulnerabilities and threats.
- Integrates current and historical information to **show trends in the behavior of mobile assets and networks** that highlight anomalies.
- **Interfaces to a variety of wireless discovery and security tools** to provide users the flexibility to use MeerCAT with their preferred tools.

1.3 What are MeerCAT's Key Features & Functions?

- **Geo-locates Wireless Devices.** MeerCAT visualizes detected wireless devices and their status on 3D geographic maps, topographic satellite imagery and imported floor plans. Users can navigate anywhere on the globe down to street and building views.
- **Generates Network Topology Maps.** MeerCAT creates a topological view of detected wireless networks to understand the impact of wireless vulnerabilities and threats. Users can 'see' the detected access points and clients connected to them.
- **Visually Captures Wireless Device Classification and Security Events.** MeerCAT's color-coded and user-customizable iconographic representation of device classification and security status allows users to immediately identify wireless devices that present risks to their networks. Device details include the SSID, location coordinates, encryption, type, and configuration.
- **Maps Access Point Coverage and Channels.** MeerCAT generates wireless coverage maps based upon the location and RF signal strength of detected access points from war drives. It displays RF signal coverage areas to help users identify interference by neighboring networks and unauthorized stations, and signal spillage in unsecured perimeters.
- **Charts Channel Usage.** MeerCAT charts the RF channel distribution for all detected networks. A histogram displays the frequency distribution of access points on each channel to determine potential interference.
- **Displays Events and Changes.** MeerCAT users can interactively compare the results of war drives with comparative views between two points in time, such as before and after

remediation. Geospatial and topological views allow users to track wireless asset movement and state changes over time.

- **Helps Analyze Device Behavior Over Time.** MeerCAT users can benefit from the ability to analyze the activity of suspicious wireless devices over time. Events and trends can be viewed over days, weeks, or even months to help improve network security posture, assist in forensic investigation and ensure policy compliance.
- **Visualizes Communication Flows.** MeerCAT's wireless network traffic visualization improves the visibility of network performance and security concerns. The visual analytic tool processes packet capture files and visually aggregates network traffic and wireless packet flow.
- **Coordinates Views for Investigation.** MeerCAT users can drill down from any window view for additional details about detected wireless networks and clients. Coordinated views allow users to quickly select a device of interest in one MeerCAT window and highlight the device in all other views for various perspectives.
- **Supports Data Filtering.** MeerCAT enables users to view, analyze, and filter wireless discovery and security data by a range of variables including the operating channel, SSID, asset, security policies, or events.
- **Helps Assess Risks.** MeerCAT users can assign missions to devices to help assess security risks due to network vulnerabilities and threats.
- **Generates Reports.** MeerCAT auto-generates a range of reports to present the results of an audit or security analysis, such as in Word or Power Point. MeerCAT also allows users to copy a MeerCAT view and place on a clipboard, export to an image file, drag and drop to other applications, and e-mail to colleagues and decision makers.
- **Delivers Out-of-the-Box Integration.** MeerCAT's data integration with wireless discovery and other security tools allow users to get immediate visual results from site surveys and security audits.

2 Getting Help With MeerCAT

2.1 MeerCAT Technical Support

All technical inquiries and bug reports can be submitted via email to meercat-support@securedecisions.com.

2.2 MeerCAT Feedback and Additional Information

Applied Visions, Inc. welcomes and encourages feedback on its products from its customers. Please submit your product inputs, user requirements and feedback to meercat@securedecisions.com.

2.3 Licensing

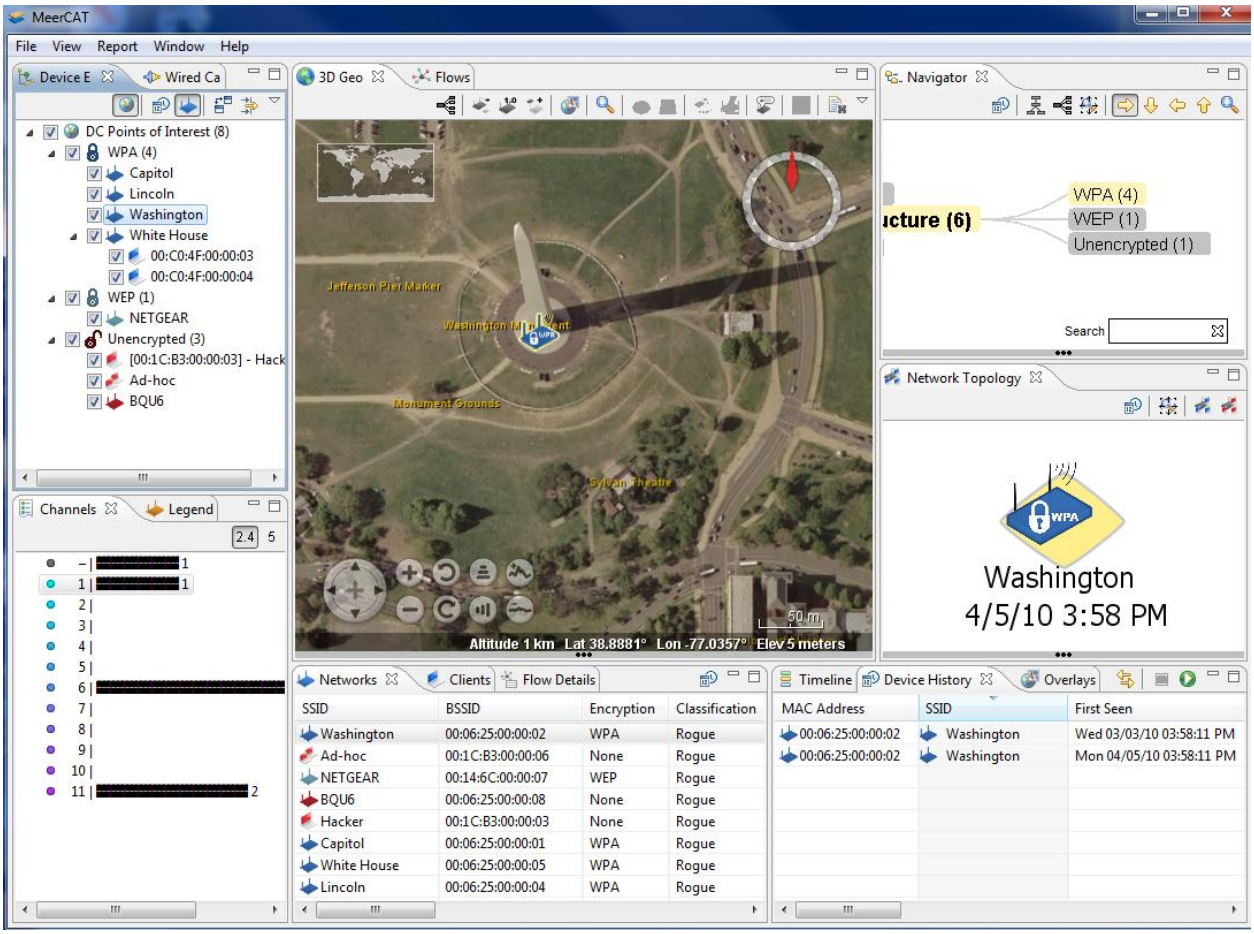
The MeerCAT software is distributed with license key(s) for each qualified licensed user in your organization. Please refer to your MeerCAT Software License Agreement for terms and conditions. If you require additional licenses, please contact Applied Visions, Inc. at meercat@securedecisions.avi.com.

3 Accessing and Navigating MeerCAT

3.1 Controlling MeerCAT

Coordinated Views

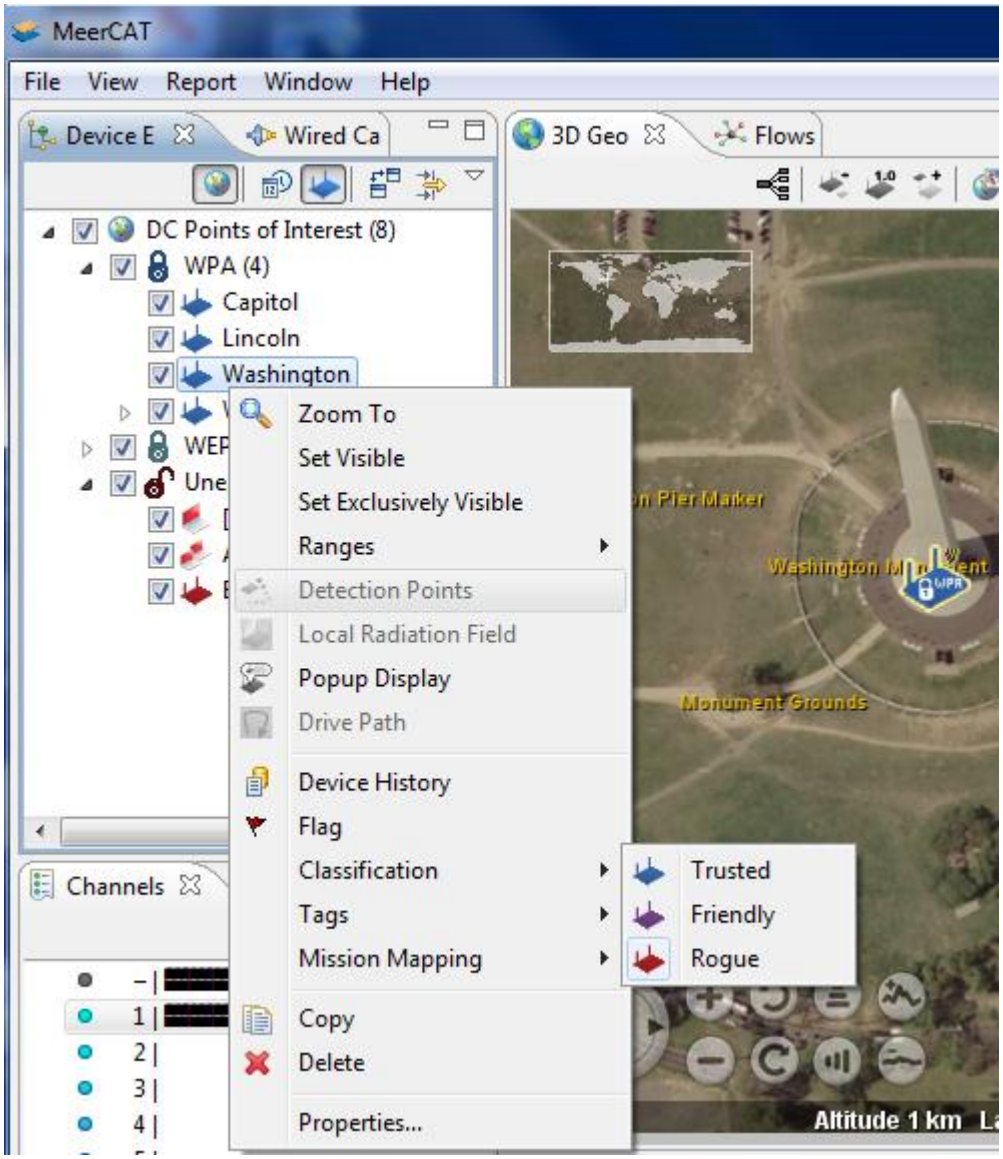
Interactions between two or more views in the MeerCAT workspace are coordinated through MeerCAT's highlighting features. Selecting data in any view highlights the data in yellow in the other views.



By placing different views in separate monitors (by dragging the view title bar) the user has access to simultaneous views of summary and detailed information.

Context Menus

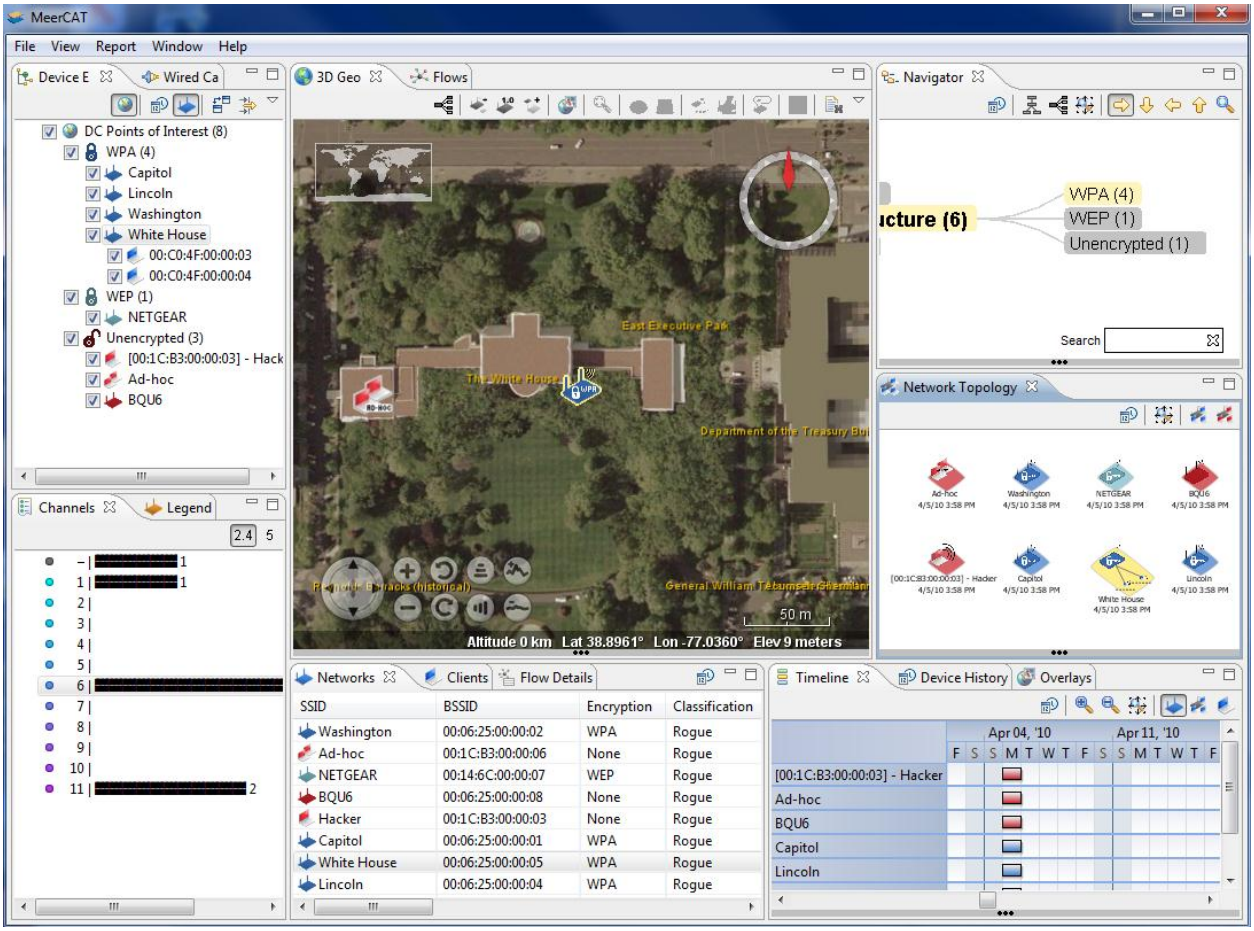
Pressing the right mouse button within some views displays contextual menus based on the data represented by a selected data element. The example below shows the contextual menu for an access point listed in the Device Explorer.



3.2 Customizing the MeerCAT Console

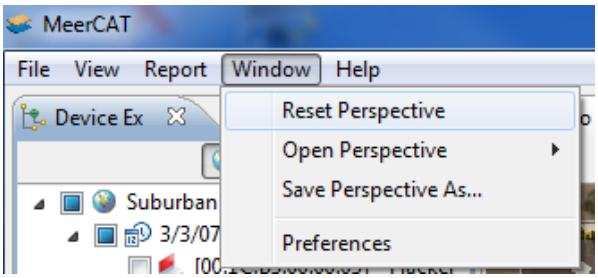
Views

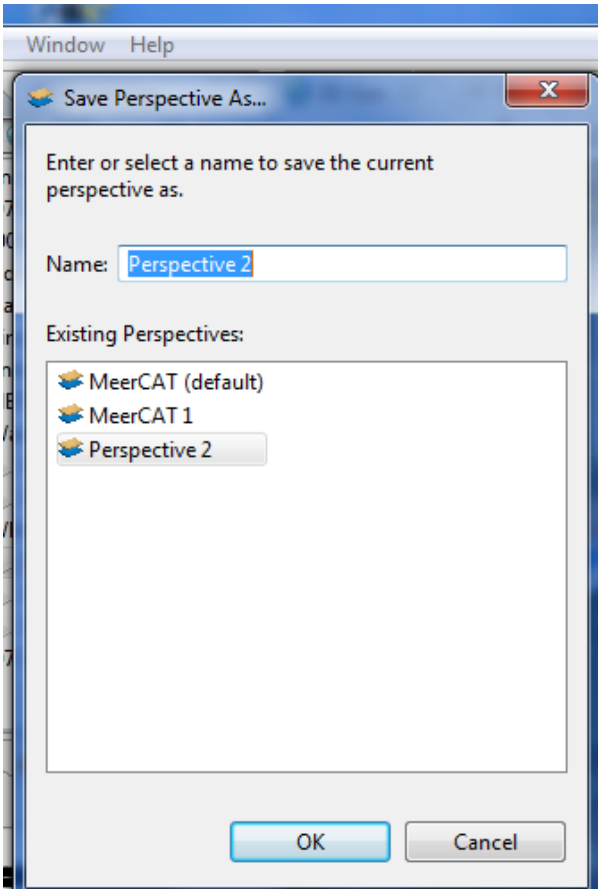
There are several windows in the default perspective of MeerCAT; each window is called a view. The individual views are described in detail in Using MeerCAT - Fundamental Tools.



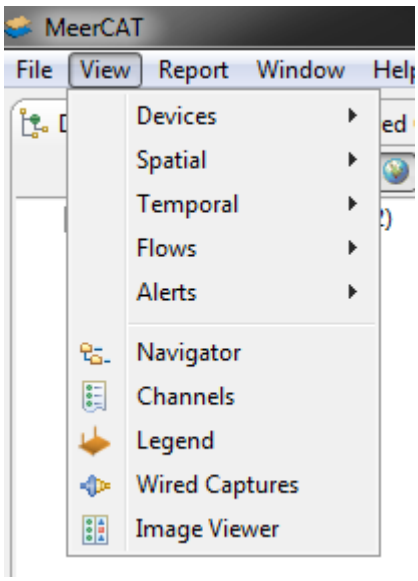
Views can be re-sized by grabbing and dragging the view bounds, or by using the minimize or maximize buttons. Views can be rearranged by dragging the view's title bar to another location. *Docking a View* is changing the location of the view in the current layout. *Detached Views* are views that are shown in a separate window with a smaller trim. When working with multiple monitors, it can be useful to put a detached view on a separate monitor. To detach a view, drag the view to the outside of the application window and release the mouse button.

The layout of the views is called a *Perspective.* You can always return to the default perspective by choosing *Window-> Reset Perspective* from the main menu bar. To save the current layout, choose *Save Perspective As*.



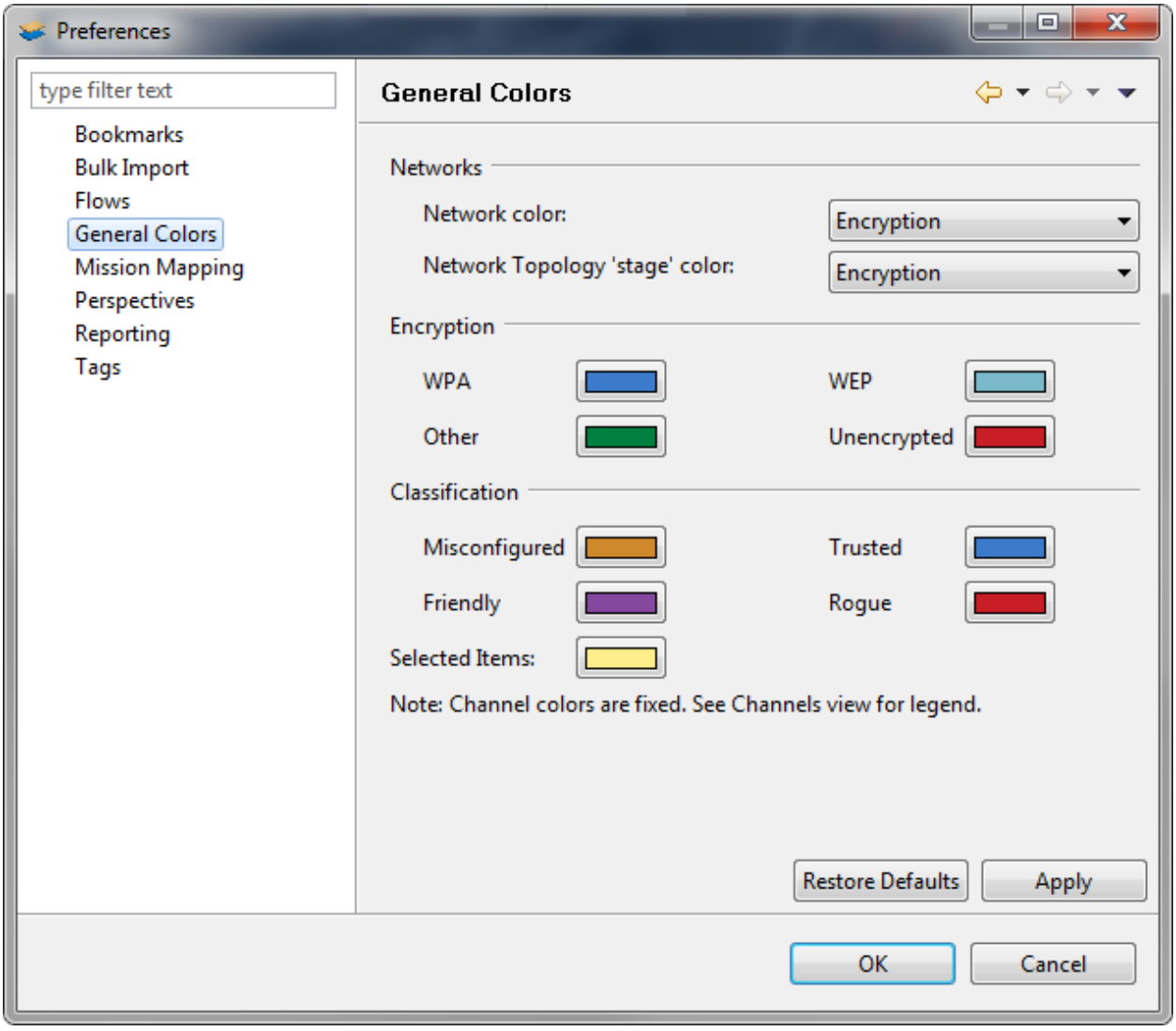


Any view that has been closed can be reopened by choosing the View menu from the main MeerCAT menu.



Preferences

Preferences allow you to customize colors, and set various options for some views.



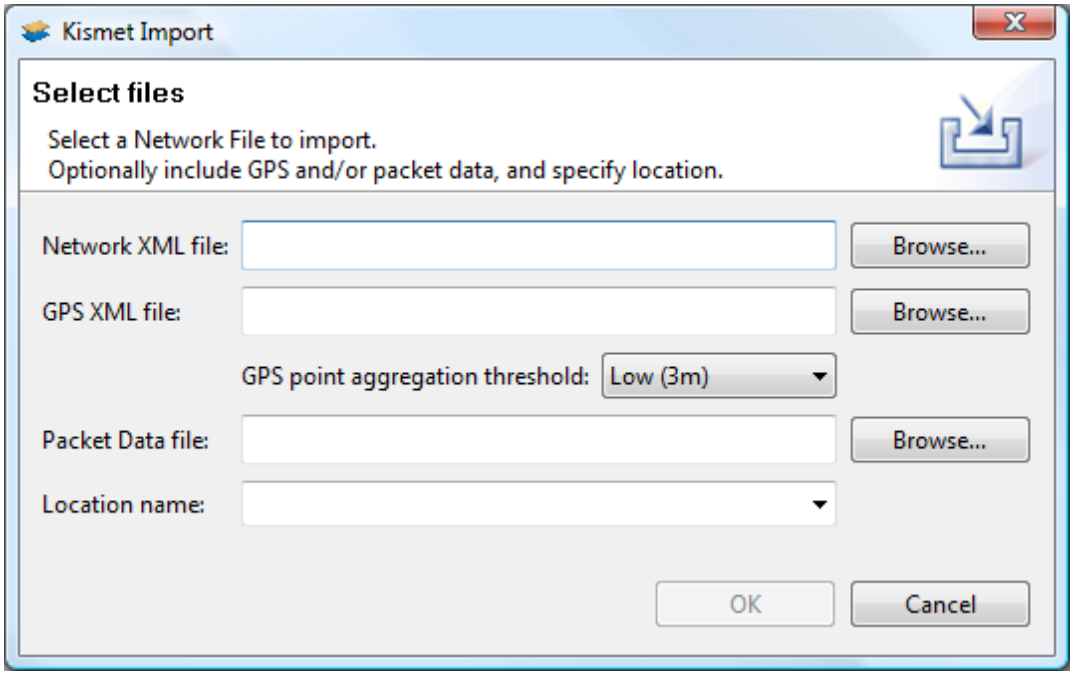
4 Importing Data Into MeerCAT

4.1 Importing Kismet Data

1. To import Kismet (including Newcore) data you have collected, or the sample data set supplied with the MeerCAT CD, select from the MeerCAT File Menu:

   File -> Import Kismet Data…

   This will launch the pop-up window:



2. On the Network XML file edit, click 'Browse', and then search for the folder with the Kismet network data formatted file (.xml or .netxml for Newcore) you want to import into MeerCAT. The default location of the sample Kismet data is: C:\Program Files\MeerCAT\demo.
3. On the *GPS XML file edit,* click 'Browse', and then search for the folder with the *Kismet GPS XML file* (.gps or .gpsxml for Newcore) you want to import into MeerCAT. This file is optional, but if selected will provide more analysis on the location of devices, such as range-based displays, like the radiation field.

   The MeerCAT database supports the storage of large number of data files and high performance data queries to quickly view and compare multiple wardrives. Nevertheless, you can choose to aggregate GPS detection points that are close to each other, in order to minimize the number of points that are stored in the database. The default setting is 3 meters; this means that if two points are less than 3 meters apart, they will be combined and treated as one point. Increasing this threshold will allow

more points to be combined, and reduce the number of points that need to be stored. If you have a very long detection run you may wish to increase this threshold in order to reduce the time it takes to import the data.

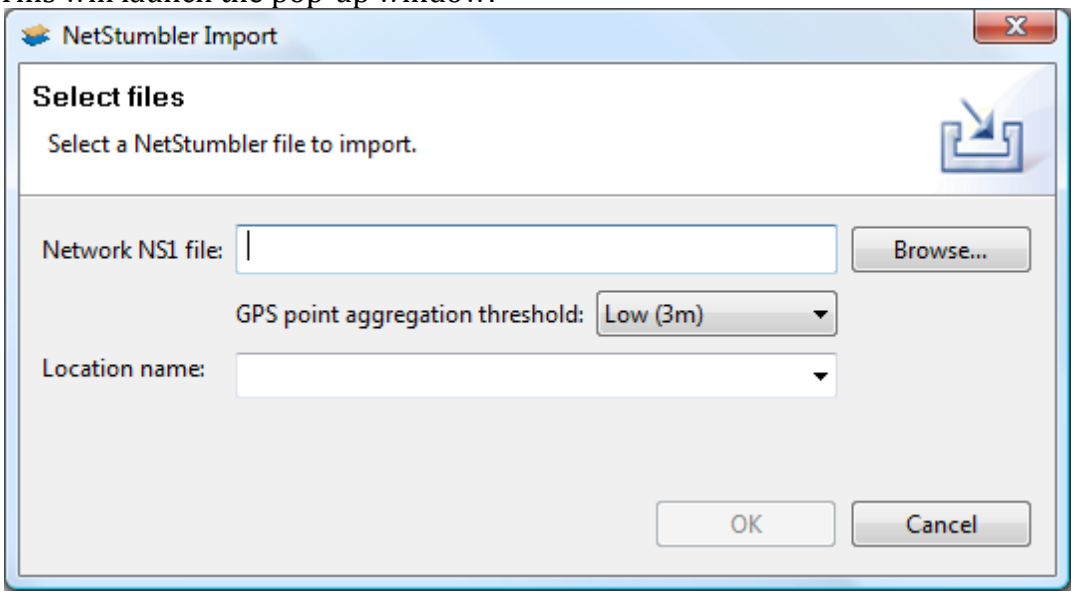
4. On the *Packet Data file edit,* click 'Browse', and then search for the folder with the *Kismet Packet Data file* (.pcap, .dump, or .pcapdump) you want to import into MeerCAT. This file is optional, but if selected will provide data for the Flows and Flow Details packet views.
5. On the *Location name edit* enter the name of the location you would like to import the data into, such as the name of the site or building that was scanned. If you perform subsequent scans of the same location, you should select that location in the dropdown menu. If no location is specified, the data will get added to an 'Unspecified Location' entry.
6. Once you have selected the file, click 'OK' to import the data into the *MeerCAT database.*
7. To *import more than one file,* repeat Steps 1-5 above for each file you choose to import for analysis.

4.2 Importing NetStumbler Data

1. To import NetStumbler data you have collected, select from the *MeerCAT File Menu*

   File -> Import NetStumbler Data…

   This will launch the pop-up window:



2. On the *Network NS1 file edit,* click 'Browse', and then search for the folder with the *NetStumbler data formatted file* (.ns1) you want to import into MeerCAT.

The MeerCAT database supports the storage of large number of data files and high performance data queries to quickly view and compare multiple wardrives. Nevertheless, you can choose to aggregate GPS detection points that are close to each other, in order to minimize the number of points that are stored in the database. The default setting is 3 meters; this means that if two points are less than 3 meters apart, they will be combined and treated as one point. Increasing this threshold will allow more points to be combined, and reduce the number of points that need to be stored. If you have a very long detection run you may wish to increase this threshold in order to reduce the time it takes to import the data.

3. On the *Location name edit* enter the name of the location you would like to import the data into, such as the name of the site or building that was scanned. If you perform subsequent scans of the same location, you should select that location in the dropdown menu. If no location is specified, the data will get added to an 'Unspecified Location' entry.
4. Once you have selected the file, click 'OK' to import the data into the *MeerCAT database.*
5. To *import more than one file,* repeat Steps 1-3 above for each file you choose to import for analysis.

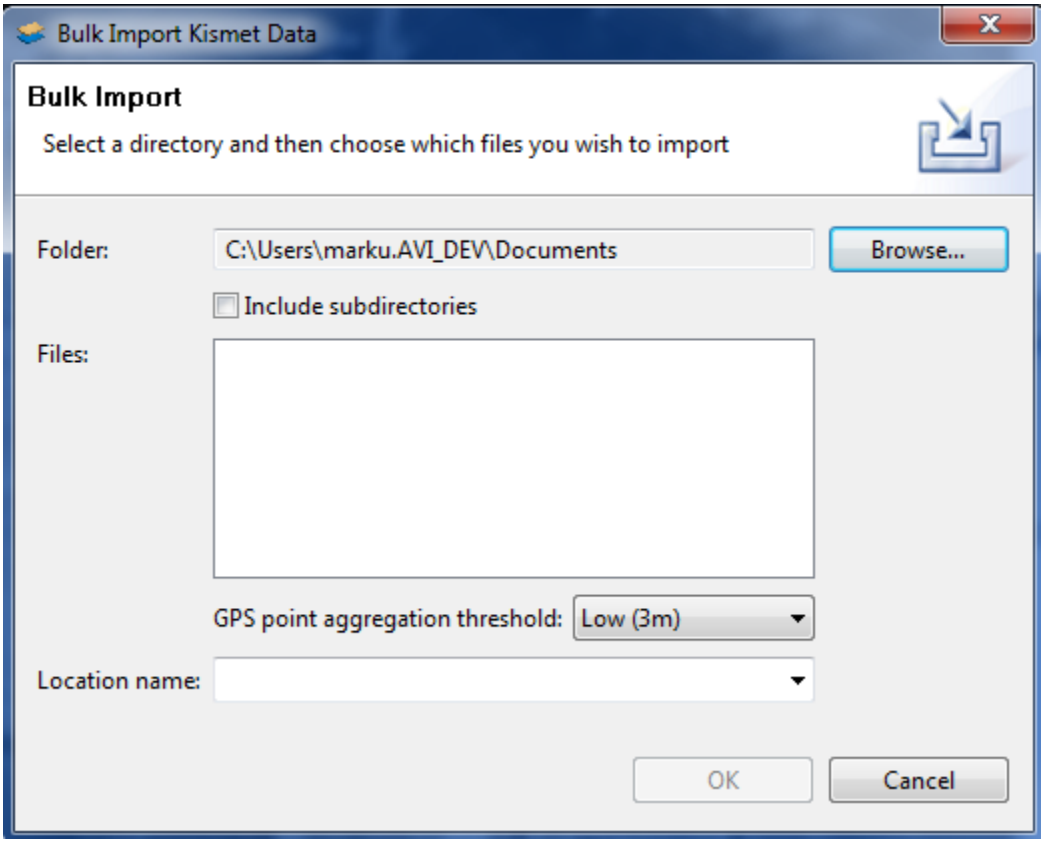
Note: NetStumbler only reports no encryption or WEP encryption. Devices may be a higher encryption, but only show as WEP. Also, NetStumbler does not collect client information nor does it collect packet data. Therefore the Network Topology view will be limited and the Flows and Flow Details views cannot be used.

4.3 Bulk Import Kismet Data

MeerCAT can import multiple Kismet data files in a single command. Access this feature through the *MeerCAT File Menu*:

File -> Bulk Import Kismet Data …

This will launch the pop-up window:



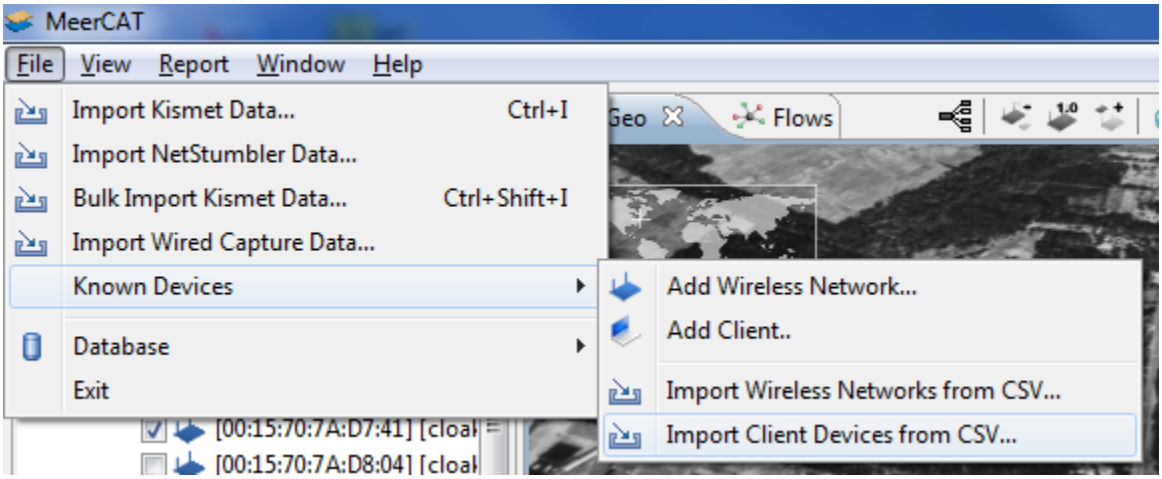
The Include subdirectories checkbox allows MeerCAT to search subdirectories for Kismet data to import.

The Location name can be entered manually, or, if an existing location is associated with the detection run, it can be selected from the dropdown.

4.4 Known Devices

MeerCAT allows you to add known devices, which serve as a baseline to alert MeerCAT users of unexpected changes, such as misconfigured devices or new devices that were not previously identified. This information is critical in defending one's network and enforcing security policies.

The Known Devices submenu can be selected from the *MeerCAT File Menu*.



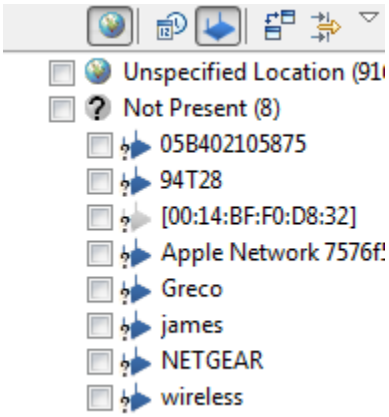
Manually Adding Known Devices

Known Networks

To add a known Network, select from the MeerCAT File Menu:

File -> Known Devices -> Add Wireless Network…

This will open a properties dialog where you can fill in the expected information for the network. If the specified network has been detected, the information will be applied to it, otherwise it will appear as "Not Present" as depicted below.

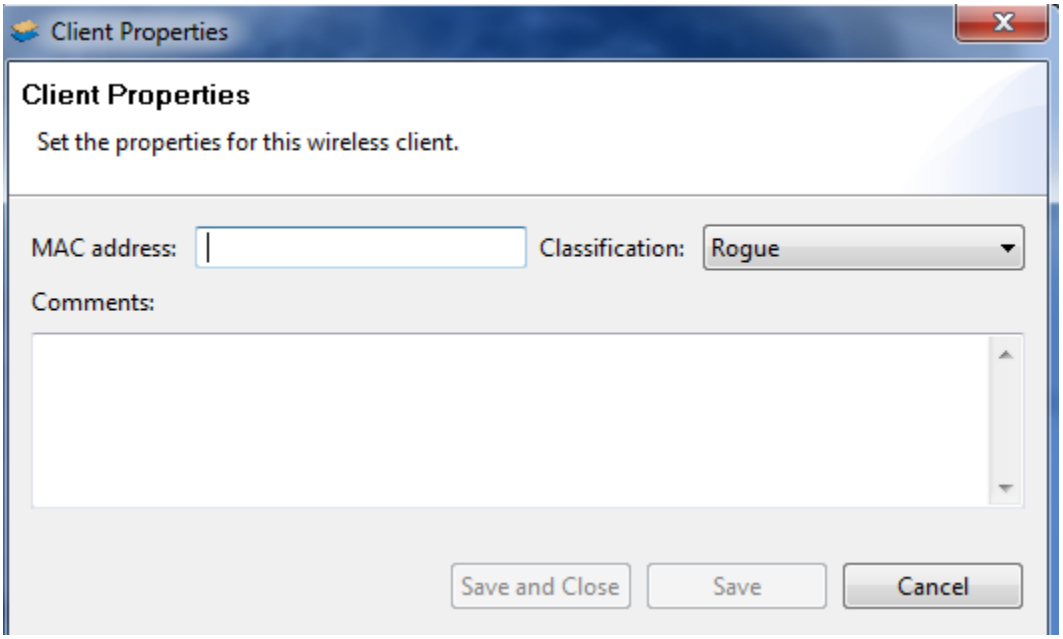


Known Clients

To add a known client device, select from the *MeerCAT File Menu*:

File -> Known Devices -> Add Client…

This will open a properties dialog where you can fill in the expected information for the client. The information will be applied to any instances of the client that have been detected or that are detected in the future.



Importing Known Devices from a CSV File

MeerCAT also supports import of CSV (Comma Separated Values) files. Its purpose is to import a list of known devices into MeerCAT.

1. To import a CSV file, select from the **MeerCAT File Menu**:

   File -> Known Devices -> Import Wireless Network [Client] from CSV ….

This will launch a browser window to locate and select the CSV file to import.

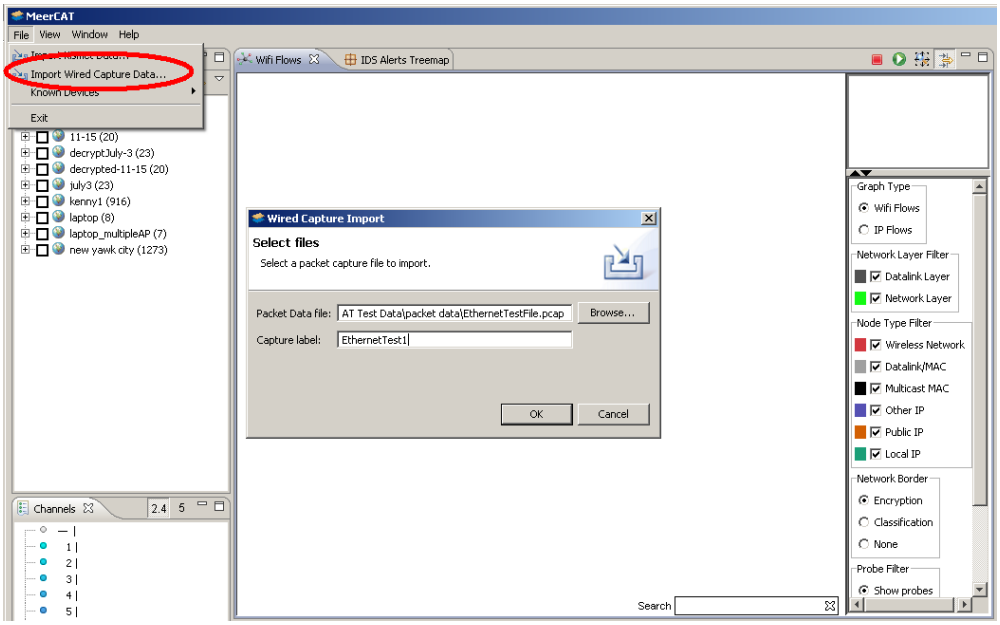
> ***Tip 1**: **Sample CSV files** are provided on the MeerCAT CD.*
>
> ***Tip 2:** The expected **order of the CSV file fields** are as follows:*
> *Known Networks: SSID, BSSID, Classification (trusted, friendly, rogue), Channel, Type (infrastructure, ad-hoc, probe), Max Rate, Encryption (WPA, WEP, None), Cloaked*
> *Known Clients: MAC address, Classification (trusted, friendly, rogue)*
>
> ***Tip 3**: Users can **manually redefine the classification of wireless devices** or set the 'baseline expected configuration' of known devices in the Device Explorer.*

2. To **import more than one CSV file** (for example, to import a CSV file for wireless networks, and a separate CSV file for wireless clients), repeat Step 1 for each file.

4.5 Importing Wired Capture Data

MeerCAT allows users to import Ethernet packet captures for limited use in some views,

namely in the Flow Details View and the IP flow graph type of the Flows View.



To import a wired (Ethernet) capture, click File on the MeerCAT menu and select "Import Wired Capture Data…" This will bring you to an import dialog as illustrated above.

5 Using MeerCAT – Fundamental Tools

5.1 MeerCAT Console

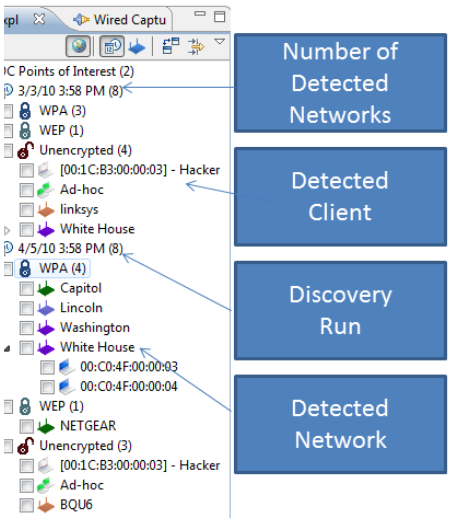
The MeerCAT Console provides multiple coordinated views of the same data for faster incident investigation. You can select a device of interest in one MeerCAT window, which will highlight the device in all other views to provide you various perspectives. These views are described in this chapter.

5.2 Device Explorer View

The Device Explorer view shows the imported *discovery runs* and lists the detected networks and connected clients for each run. It enables you to view, analyze, and filter wireless discovery and security data by a range of variables such as the device type, manufacturer, SSID and other device property. The Device Explorer also provides a number of tools for coordinating other MeerCAT Console views and identifying the attributes of detected wireless devices:

1. **Expand each *discovery run* to display the individual networks detected.**

   Click on the '+' symbol adjacent to each session run to expand the view of detected networks.



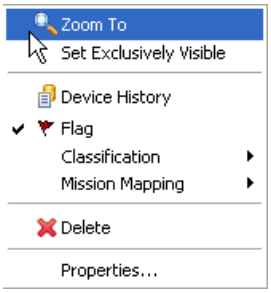
   > ***Tip 1:** **Number of detected networks** in a discovery run is the number adjacent to the run.*
   >
   > ***Tip 2: Networks with unknown locations** are annotated with a '?' mark on the device icon.*

2. **Expand each discovered network to show the discovered clients connected to that network.**

   Click on the '+' symbol adjacent to each network to expand the view of detected connected clients.

3. **Update the attributes of a device**

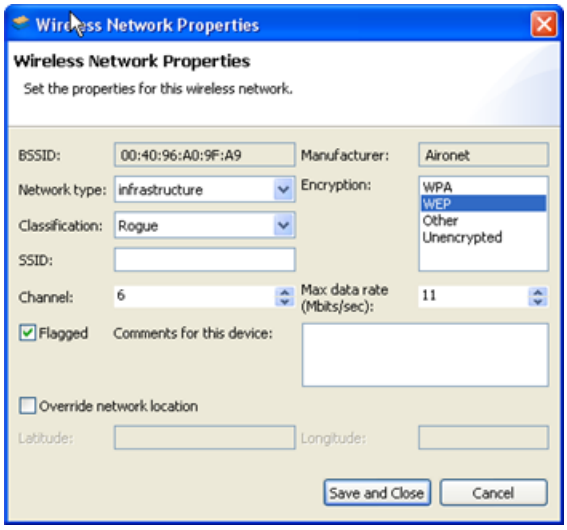
   Users can quickly **update device properties** after an analysis of a discovery session. For example, a device initially classified as rogue may be a neighboring network that is friendly, which the user may then reclassify.



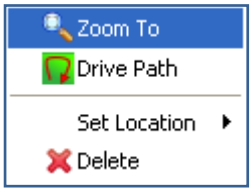
   Right-Click [client]

4. **Update the attributes of a wireless network**

   Right-Click [network]->Properties



5. **Zoom in on a discovery run or network for all MeerCAT Views**



Right-Click [discovery run or network]->Zoom To

-or-

Double-Click [discovery run, network or device]

> ***Tip 4: Delete discovery run data*** *by:*
> *Right Click [on Discovery Run in Device Explorer] > Select Delete'.*

Toolbar

The toolbar of the Device Explorer view contains the following buttons:

Toggle Detection Run Location Grouping

Determines whether or not to group the networks and detection runs by the "location" that was specified when the data was imported.

Detection Runs

Shows a list of detection runs, and expanding each detection run will show the individual devices that were detected on that run.

Networks

Displays the latest history for all devices detected across all detection runs. The user can then select a network and look at the "Device History" view to see the instances when the device was seen (if "Link With Selection" is enabled in that view).

If a particular historical instance is selected within the Device History view, that instance will be shown instead of the latest (except in the Network and Clients table views).

Compare Detection Runs

Allows the user to select detection runs and compare them by showing only the devices that changed from one detection run to another by looking at several attributes.

Filter Wireless Networks

Shows only wireless devices that fit criteria specified by the user in the selection window.

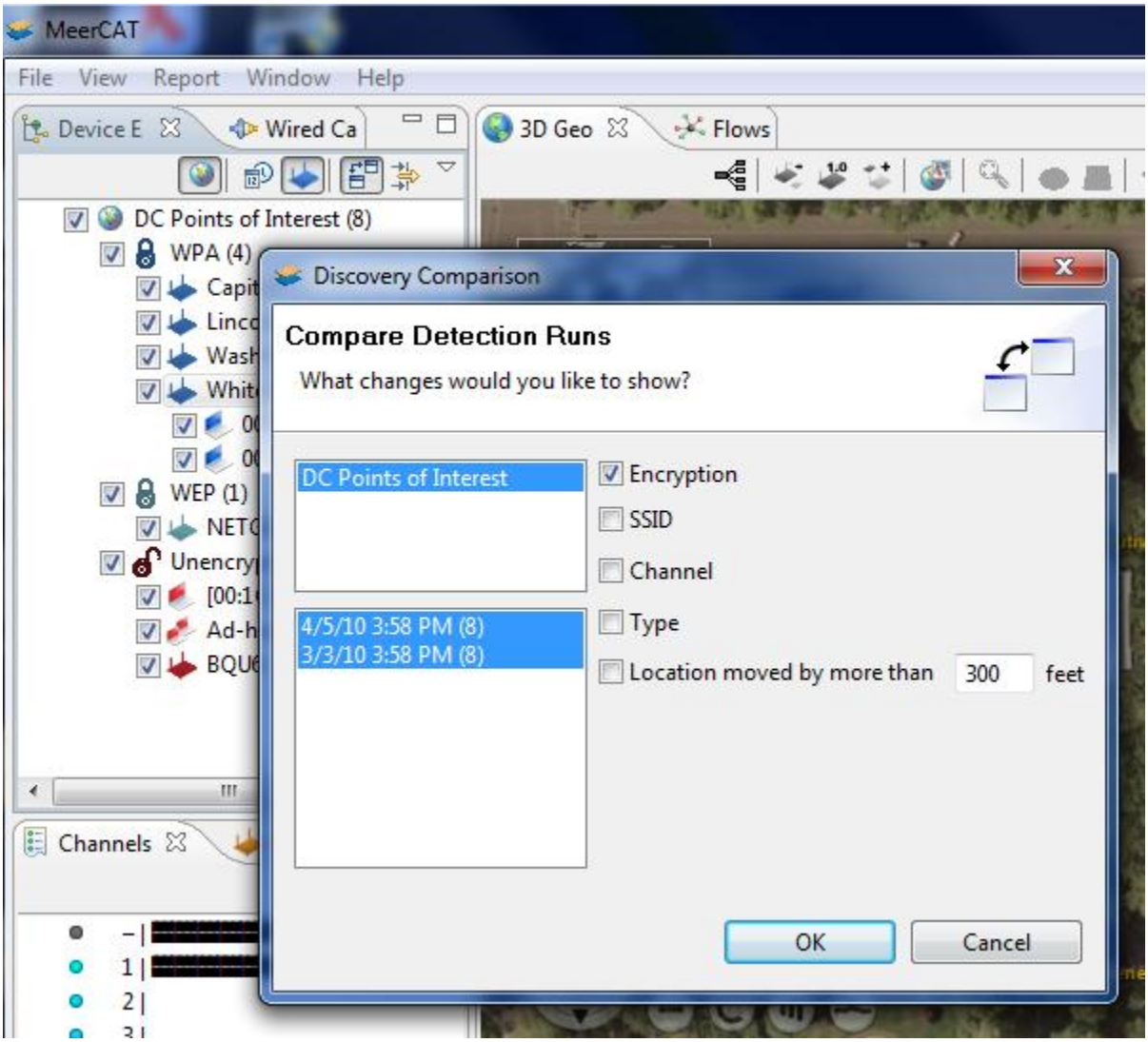
View Menu

Allows user to change the order that the devices show up ("Sorting") and optionally group the devices by a criterion (e.g., grouped by encryption type). You can also export or import the list of items that are currently checked off in the device explorer.

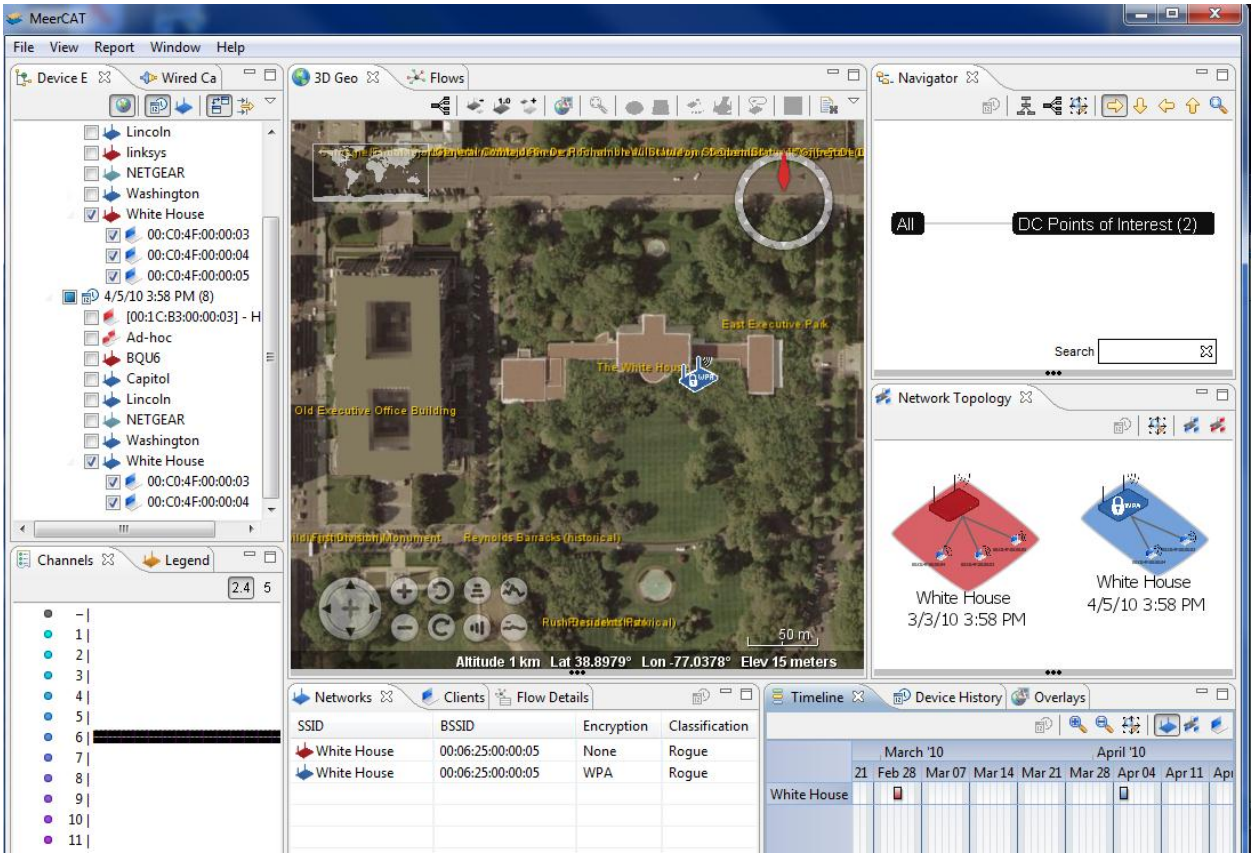
Illustrative Windows

With Compare Detection Runs you can see if a particular network has changed its encryption, SSID, channel, type, or location, which is beneficial in alerting you to security concerns or validating whether a corrective action has resolved an issue.

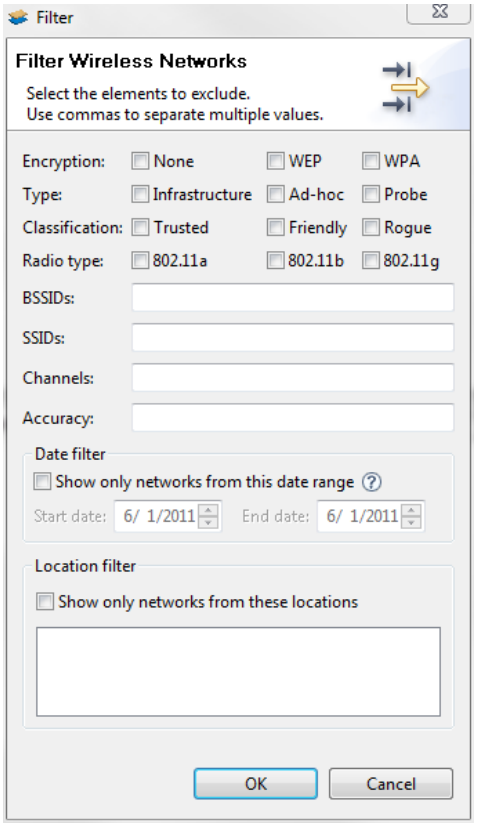
Choose the detection runs you want to compare by holding the SHIFT or CTRL key down to select them. Check off the attributes you want to compare.



The devices that remain will show the comparisons you have selected.

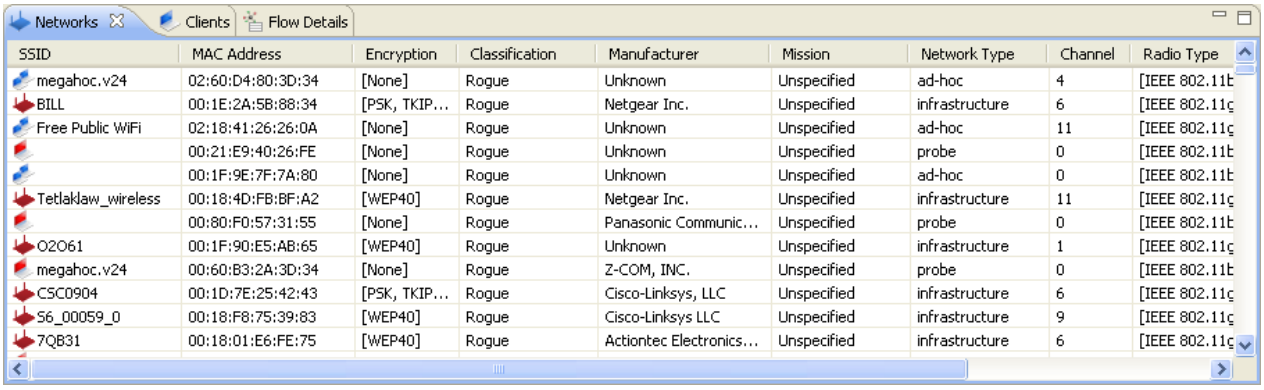

MeerCAT
File View Report Window Help
Device E
Wired Ca
Lincoln
linksys
NETGEAR
Washington
White House
00:C0:4F:00:00:03
00:C0:4F:00:00:04
00:C0:4F:00:00:05
4/5/10 3:58 PM (8)
[00:1C:B3:00:00:03] - H
Ad-hoc
BQU6
Capitol
Lincoln
NETGEAR
Washington
White House
00:C0:4F:00:00:03
00:C0:4F:00:00:04
Channels
Legend
3D Geo
Flows
East Executive Park
Old Executive Office Building
50 m
Altitude 1 km Lat 38.8979° Lon -77.0378° Elev 15 meters
Navigator
All
DC Points of Interest (2)
Search
Network Topology
White House
3/3/10 3:58 PM
White House
4/5/10 3:58 PM
Networks
Clients
Flow Details
SSID
BSSID
Encryption
Classification
White House
00:06:25:00:00:05
None
Rogue
White House
00:06:25:00:00:05
WPA
Rogue
Timeline
Device History
Overlays
March '10
April '10
21 Feb 28 Mar 07 Mar 14 Mar 21 Mar 28 Apr 04 Apr 11
White House

The Wireless Network filter shows only wireless devices that fit the criteria specified by the user in the selection window.



5.3 Networks View

The Networks View offers another tool to simplify wireless device management and security, and helps you identify network devices based on their properties including their MAC address, SSID, vendor, security, or channel. With the Network Device Table you can easily browse and sort through the various categories of detected devices to quickly validate unauthorized devices.


Networks
Clients
Flow Details
SSID | MAC Address | Encryption | Classification | Manufacturer | Mission | Network Type | Channel | Radio Type
megahoc.v24 | 02:60:D4:80:3D:34 | [None] | Rogue | Unknown | Unspecified | ad-hoc | 4 | [IEEE 802.11b
BILL | 00:1E:2A:5B:88:34 | [PSK, TKIP... | Rogue | Netgear Inc. | Unspecified | infrastructure | 6 | [IEEE 802.11g
Free Public WiFi | 02:18:41:26:26:0A | [None] | Rogue | Unknown | Unspecified | ad-hoc | 11 | [IEEE 802.11g
00:21:E9:40:26:FE | [None] | Rogue | Unknown | Unspecified | probe | 0 | [IEEE 802.11b
00:1F:9E:7F:7A:80 | [None] | Rogue | Unknown | Unspecified | ad-hoc | 0 | [IEEE 802.11b
Tetlaklaw_wireless | 00:18:4D:FB:BF:A2 | [WEP40] | Rogue | Netgear Inc. | Unspecified | infrastructure | 11 | [IEEE 802.11g
00:80:F0:57:31:55 | [None] | Rogue | Panasonic Communic... | Unspecified | probe | 0 | [IEEE 802.11b
O2O61 | 00:1F:90:E5:AB:65 | [WEP40] | Rogue | Unknown | Unspecified | infrastructure | 1 | [IEEE 802.11g
megahoc.v24 | 00:60:B3:2A:3D:34 | [None] | Rogue | Z-COM, INC. | Unspecified | probe | 0 | [IEEE 802.11b
CSC0904 | 00:1D:7E:25:42:43 | [PSK, TKIP... | Rogue | Cisco-Linksys, LLC | Unspecified | infrastructure | 6 | [IEEE 802.11g
S6_00059_0 | 00:18:F8:75:39:83 | [WEP40] | Rogue | Cisco-Linksys LLC | Unspecified | infrastructure | 9 | [IEEE 802.11g
7QB31 | 00:18:01:E6:FE:75 | [WEP40] | Rogue | Actiontec Electronics... | Unspecified | infrastructure | 6 | [IEEE 802.11g

Toolbar

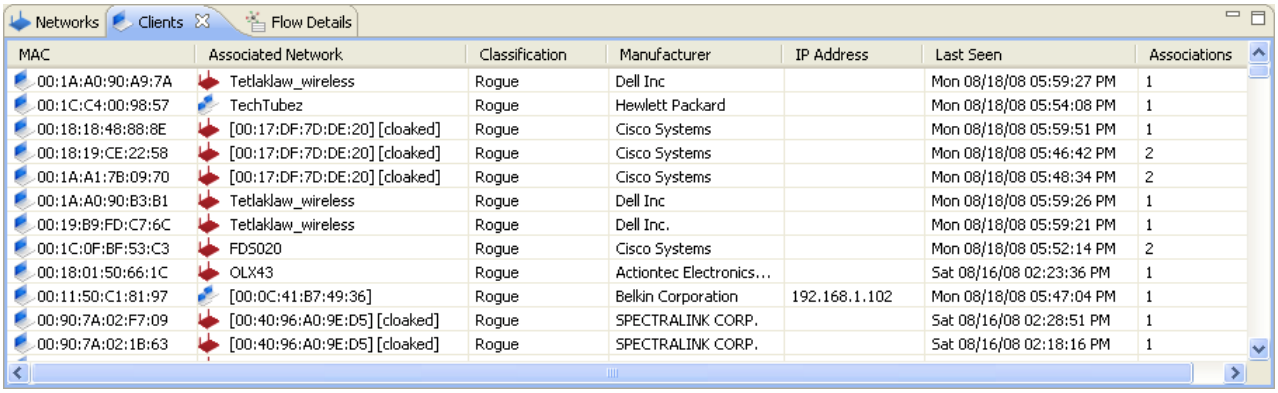
The toolbar of the Networks view contains the following button:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of the particular wireless network(s) in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s).

5.4 Clients View

The Clients View is a companion to the Networks View, offering another tool to simplify wireless device management and security. Clients View helps you identify individual client devices based on their properties including their MAC or IP address, associated network, classification, or when they were last seen. With the Clients View you can easily browse and sort through the various categories of detected client devices to quickly validate unauthorized devices. The Associations column can be useful for finding clients that have made connections to multiple networks.



MAC	Associated Network	Classification	Manufacturer	IP Address	Last Seen	Associations
00:1A:A0:90:A9:7A	Tetlaklaw_wireless	Rogue	Dell Inc		Mon 08/18/08 05:59:27 PM	1
00:1C:C4:00:98:57	TechTubez	Rogue	Hewlett Packard		Mon 08/18/08 05:54:08 PM	1
00:18:18:48:88:8E	[00:17:DF:7D:DE:20] [cloaked]	Rogue	Cisco Systems		Mon 08/18/08 05:59:51 PM	1
00:18:19:CE:22:58	[00:17:DF:7D:DE:20] [cloaked]	Rogue	Cisco Systems		Mon 08/18/08 05:46:42 PM	2
00:1A:A1:7B:09:70	[00:17:DF:7D:DE:20] [cloaked]	Rogue	Cisco Systems		Mon 08/18/08 05:48:34 PM	2
00:1A:A0:90:B3:B1	Tetlaklaw_wireless	Rogue	Dell Inc		Mon 08/18/08 05:59:26 PM	1
00:19:B9:FD:C7:6C	Tetlaklaw_wireless	Rogue	Dell Inc.		Mon 08/18/08 05:59:21 PM	1
00:1C:0F:BF:53:C3	FDS020	Rogue	Cisco Systems		Mon 08/18/08 05:52:14 PM	2
00:18:01:50:66:1C	OLX43	Rogue	Actiontec Electronics...		Sat 08/16/08 02:23:36 PM	1
00:11:50:C1:81:97	[00:0C:41:B7:49:36]	Rogue	Belkin Corporation	192.168.1.102	Mon 08/18/08 05:47:04 PM	1
00:90:7A:02:F7:09	[00:40:96:A0:9E:D5] [cloaked]	Rogue	SPECTRALINK CORP.		Sat 08/16/08 02:28:51 PM	1
00:90:7A:02:1B:63	[00:40:96:A0:9E:D5] [cloaked]	Rogue	SPECTRALINK CORP.		Sat 08/16/08 02:18:16 PM	1

Toolbar

The toolbar of the Clients view contains the following button:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of the particular wireless network(s) in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s).

5.5 3D Geographic View

The **3D 'Geo' View** provides the tools to locate wireless networks and clients on 3D topographic satellite imagery. Users can navigate anywhere on the globe down to street and building views to locate friendly and rogue devices.

Using the 'Zoom To' tool on a discovery run in the Device Explorer as described in Device Explorer View, the coordinated 3D Geo View below that shows all the detected devices in the selected discovery run. The **3D Geo View** also provides tools to further analyze the attributes of detected wireless devices:

1. Display a **device attributes** by:

   Right Click [Device]>Show Popup Display

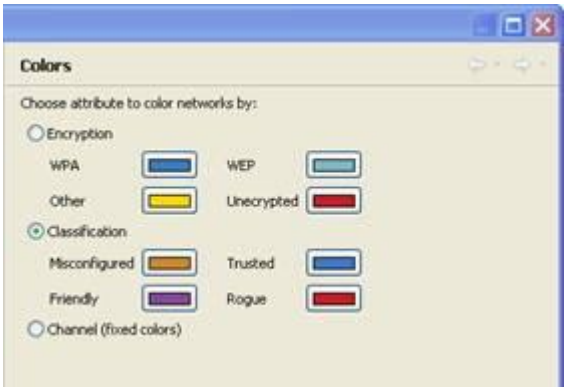
2. Invoke **Coordinated Views** to inspect wireless devices by:

   Left Click [on any device on the map]

> ***Tip 1:*** ***Encrypted devices*** *show a lock symbol.*
> ***Tip 2:*** *The* ***device encryption level*** *is displayed on the device icon (e.g., WPA or WEP).*

   This will highlight the device in the other MeerCAT Console views.

3. User customizable views are supported including the ability to **redefine the color** coding **of wireless networks**:
   a. *MeerCAT Windows Menu -> Preferences…*
   b. *Select the attribute that the device color will represent (Encryption, Classification or Channel)*
   c. *Click on any color buttons to select the color code for the selected attribute.*



> ***Tip 3****: The* ***network color*** *is preconfigured to represent device classification. The default is:*
> *Blue=Secure/Trusted Red =Unsecure/Rogue; Purple=Friendly; Orange=Misconfigured*

The **3D 'Geo' View** provides the tools to locate wireless networks and clients on 3D topographic satellite imagery. Users can navigate anywhere on the globe down to street and building views to locate friendly and rogue devices.

Using the 'Zoom To' tool on a discovery run in the Device Explorer as described in Device Explorer View, the coordinated 3D Geo View below that shows all the detected devices in the selected discovery run. The **3D Geo View** also provides tools to further analyze the attributes of detected wireless devices:

4. Display a **device attributes** by:

   Right Click [Device]>Show Popup Display

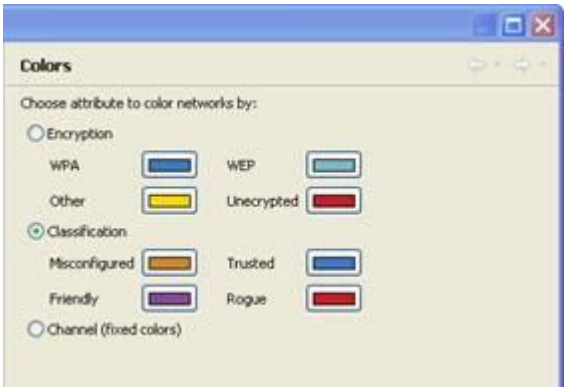
5. Invoke **Coordinated Views** to inspect wireless devices by:

   Left Click [on any device on the map]

   Tip 1: ***Encrypted devices*** *show a lock symbol.*
   Tip 2: *The* ***device encryption level*** *is displayed on the device icon (e.g., WPA or WEP).*

   This will highlight the device in the other MeerCAT Console views.

6. User customizable views are supported including the ability to **redefine the color** coding **of wireless networks**:
   a. *MeerCAT Windows Menu -> Preferences…*
   b. *Select the attribute that the device color will represent (Encryption, Classification or Channel)*
   c. *Click on any color buttons to select the color code for the selected attribute.*



Tip 3*: The* ***network color*** *is preconfigured to represent device classification. The default is:*
Blue=Secure/Trusted Red =Unsecure/Rogue; Purple=Friendly; Orange=Misconfigured

Controls

Mouse with scroll wheel:

Pan:	Left mouse button click & drag - all directions or arrow keys or double-left-click an area.
Zoom:	Use the scroll wheel on the mouse or Hold "Ctrl" and arrow up or down on the keyboard or Use + (zoom in) and – (zoom out) keys.
Tilt:	Right mouse button click & drag - up and down or Use "Page Up" and "Page Down" on the keyboard or Hold "shift" and arrow up or down on the keyboard.
Rotate:	Right mouse button click & drag - left and right (Note: Crossing the top and bottom half of the screen while rotating will change direction) or Hold "shift" and arrow up or down on the keyboard

Stop:	Spacebar
Reset Heading:	N
Reset all:	R

Single button mouse:

Pan:	Left mouse button click & drag - all directions. Left mouse button click once to center view or arrow keys or double-left-click an area.
Zoom:	Hold "Ctrl" on the keyboard and left mouse button click & drag - up and down or hold “Ctrl” and arrow up or down on the keyboard.
Tilt:	Hold "Shift" on the keyboard and left mouse button click & drag - up and down or use "Page Up" and "Page Down" on the keyboard.
Rotate:	Hold "Shift" on the keyboard and left mouse button click & drag - left and right.
Stop:	Spacebar
Reset Heading:	N
Reset all:	R

Toolbar

The toolbar of the 3D Geo view contains the following buttons:

Set Icon Display Options
Set icon display options – controls automatic aggregation / sizing of icons of the map.

Decrease icon size
Decreases the size of all the icons on the map by half.

Set icon size to 1.0x
Sets all icons back to their original size.

Increase icon size
Increases the size of all the icons on the map by 2x.

Add Image Overlay
Invokes the “image overlay” dialog.

Zoom to the Location on the map
Enabled when one or more networks are selected – zooms to those networks when clicked.

Show circular area depicting the longest distance a network was detected

Enabled when one or more networks are selected – draws a circle around the network showing the max detection radius.

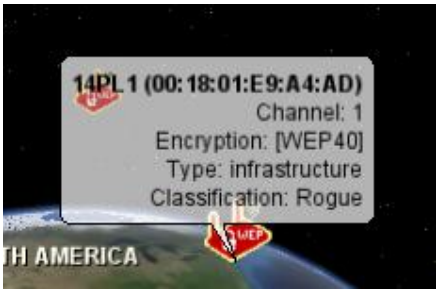
Toggle polygonal area of points where a network was detected
Enabled when one or more networks are selected – draws a polygon (convex hull) enclosing all the points where the network is detected.

Show all points where the network was detected
Enabled when one or more networks are selected – shows all the points that a network was detected.

Toggle a display of the access point's interpolated signal strength
Enabled when one or more networks are selected – shows a "heatmap" which shows the signal strength around the network by interpolating from the detection points.

Toggle a display of the client's interpolated signal strength
Enabled when one or more clients are selected – shows a "heatmap" which shows a client's signal strength by interpolation.

Show extra information about an item on the map
Enabled when one or more networks are selected – shows a callout with detailed information about the network(s):



Toggle display of the drive path for a detection run
Enabled when one or more detection runs are selected – draws a line depicting the drive path.

Clear Extra Display Info
Clears out all extra info on the map (annotations, range overlays

3D Specialized Controls

Additional controls are available in this View to supplement navigation within the view. These controls are shown below:

This set of controls and buttons can be found in the lower left corner of the 3D Geo View.

Directional Control

Use this control to move the 3D image left, right, up or down.

Zoom

Use these buttons to zoom in or out.

Rotation

Use these buttons to rotate the image to the left or right.

Tilt

Use these buttons to tilt the image forward or backward.

Elevation

Use these buttons to increase or decrease elevation.

5.6 Network Topology View

MeerCAT automatically constructs topological maps of the discovered networks and connected clients to help you better understand the impact of wireless vulnerabilities and threat and determine the appropriate remediation. MeerCAT helps you 'see' the detected access points and clients connected to them, including rogue and unsecure devices.

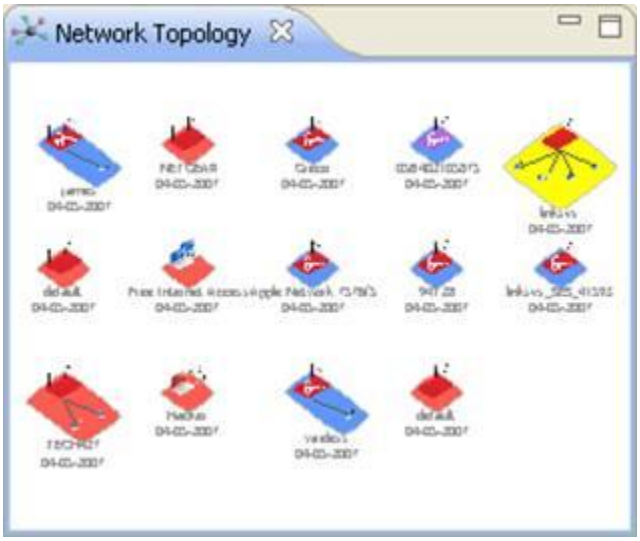
Coordinated views allow MeerCAT users to quickly spot a network of interest in the Network Topology View to help identify connected clients and potential risks for further investigation. If multiple networks are checked off in the Device Explorer, then the latest information for that network will be shown. If only one network is selected, then all histories will be shown side-by-side over time.

*Tip 1: The **network 'stage' color** is preconfigured to represent the network security state, where the default coding is:*

Red = unencrypted
Blue = encrypted

Stages highlighted in yellow indicate the device has been user-selected for coordinated views.

The 'stage' is user configurable MeerCAT Windows Menu>Preferences…



MeerCAT provides tools to analyze device attributes in the Network Topology View:

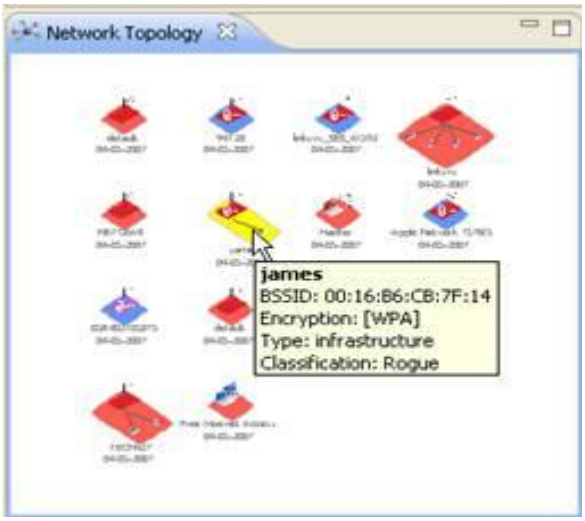
1. Place the mouse cursor over [any device]

   A '**tooltip**' will appear with the devices attributes.

2. Invoke **Coordinate views** by:

   Left Click [any device]

   The device will be highlighted in all MeerCAT Console views.



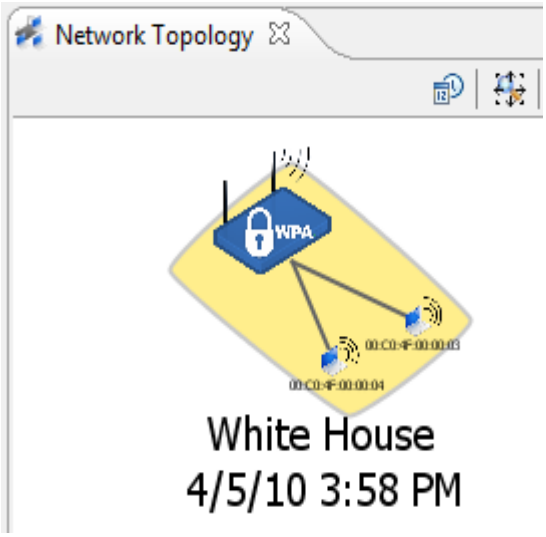
***Tip 2**: There are a number of tools to navigate in the Network Topology View:*

*a) To **center a network of interest** in Network Topology View*

Left Click and hold (anywhere in white space around network icon)> Move mouse to area

*b) To **'Zoom In/Out'** on any network by:*

Right Click and hold> Move mouse forward and back



Toolbar

The toolbar of the Network Topology view contains the following buttons:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

Zoom the display such that all of its contents are visible

Show only networks with clients

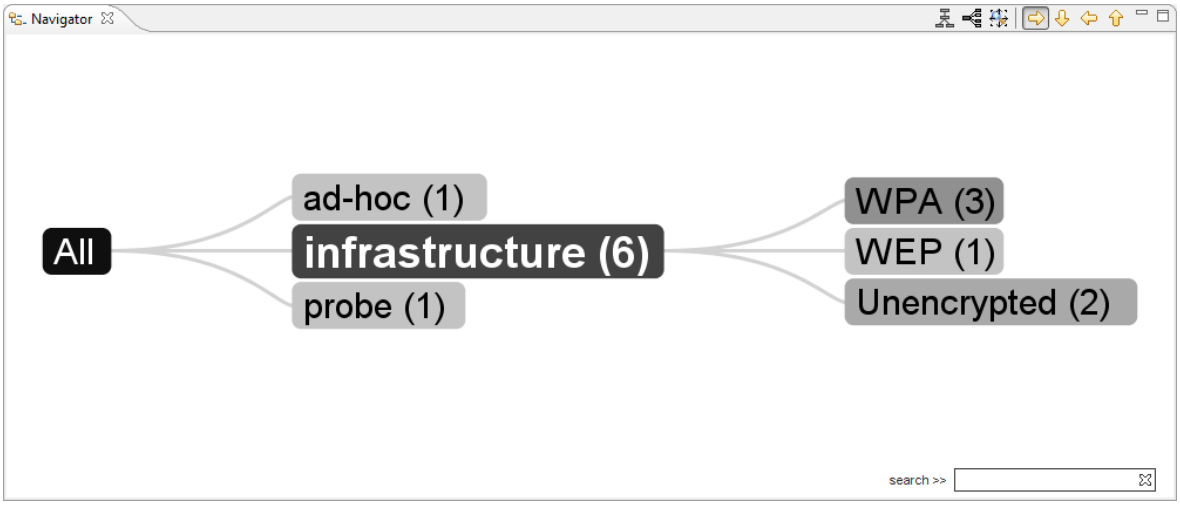
Show rogue clients connected to trusted networks and trusted clients connected to rogue networks

5.7 Navigator View

The Navigator View provides an alternative tree representation of the networks checked in the Device Explorer. The Navigator view is helpful for visualizing and navigating large amounts of data. As nodes are selected in the tree, the view changes its focus to that item, maximizing screen space.

This view also provides extensive grouping, aggregation, filtering, and searching capabilities.

In the example below, color darkness is used to indicate groups with a greater count. Alternatively, coloring can be based on packets or number of clients connected to the network. Here we see that the bulk of the networks are of type infrastructure. We know this base on the darker color and the count of 6 displayed in the label.



Selection / Highlighting

If a node has not been expanded, double clicking it will cause focus to that node and expand any available children. If an item represents a specific device in the data set, selecting it will cause it to become highlighted, and all the other views within MeerCAT will highlight that group as well. In addition, if you hold the SHIFT key and select an item, the item becomes highlighted as well as all of its children. For example, if you hold SHIFT and click to select the WPA node, all devices that have WPA enabled will become highlighted in all of the views. By holding CTRL while selecting devices, you can select several devices to become highlighted in all of the views.

Panning

Left-clicking on the display allows you to pan.

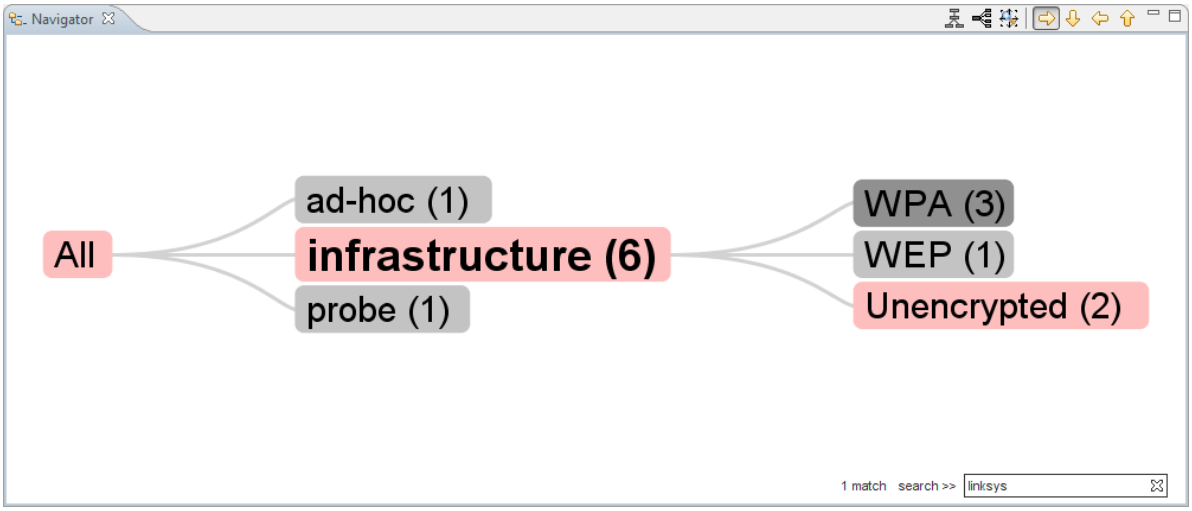
Zooming

Holding right-clicking and moving the mouse up or down causes the view to zoom out/in. Right-clicking without moving the mouse will cause the display to refit to the current window size.

Searching

The search bar in the lower right of the display allows you to query for a particular BSSID, SSID, MAC address, or other label currently in the display, such as WEP. The sample below shows that only one linksys device was found. It is unencrypted and of type infrastructure. This searching is incremental, so as you type matching nodes will be highlighted.

A right click in the search panel outside of the text editing area will pop up a list of search results if there are any. The user can then click on a search result and the navigator will expand and zoom into that particular item in the graph.



Toolbar

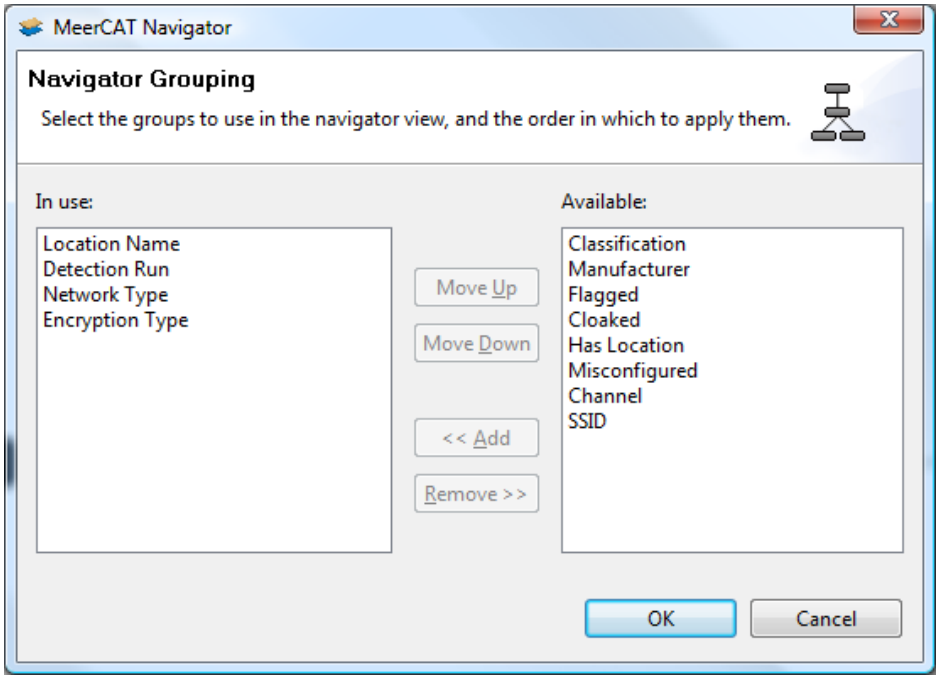
The toolbar of the Navigator view contains the following buttons:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

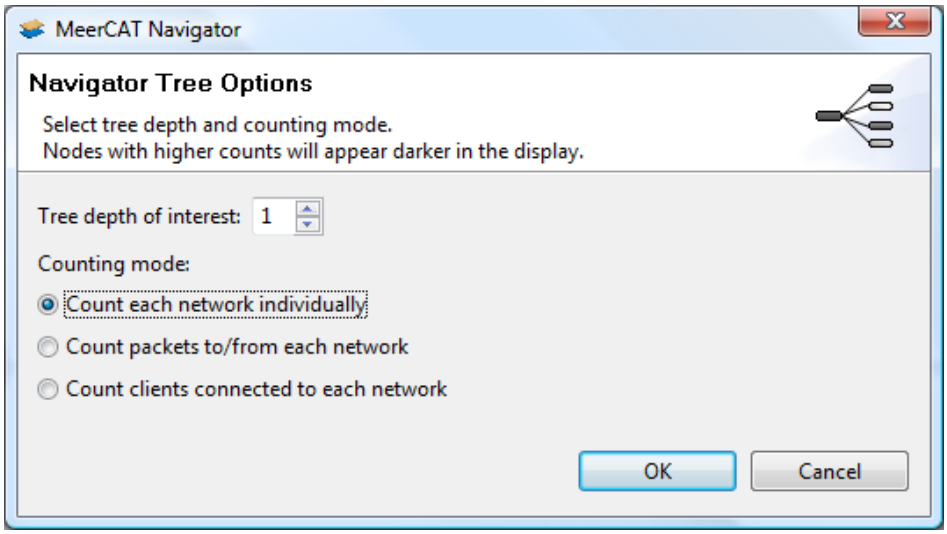
Navigator Grouping

This option allows you to set the grouping order of the tree.



Navigator Tree Options

This dialog allows you to set the depth of the tree, meaning how many children will be shown from the focused node. The dialog also allows you to select how the node should be colored, either by count, number of packet, or number of clients.

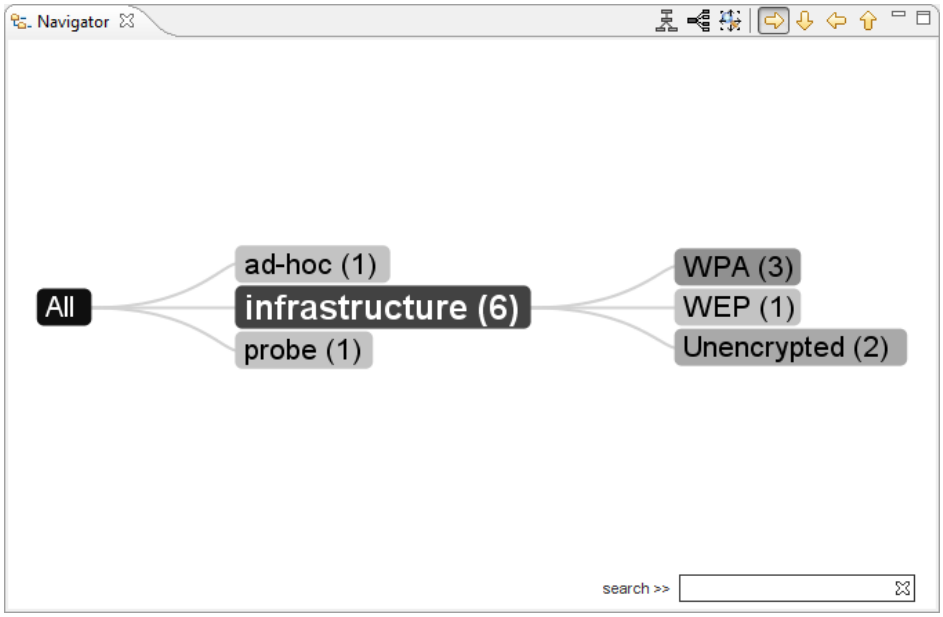

MeerCAT Navigator
Navigator Tree Options
Select tree depth and counting mode.
Nodes with higher counts will appear darker in the display.
Tree depth of interest: 1
Counting mode:
Count each network individually
Count packets to/from each network
Count clients connected to each network
OK
Cancel

Zoom to Fit

This option will refit the display to fit the size of the current display.

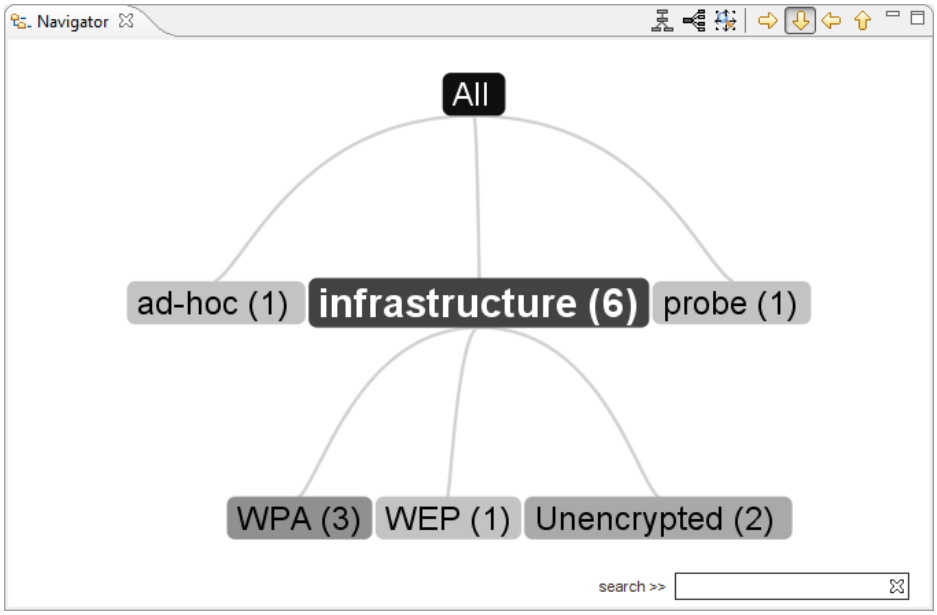
Orient Left-Right

This option will cause the display to show from left to right as shown below:



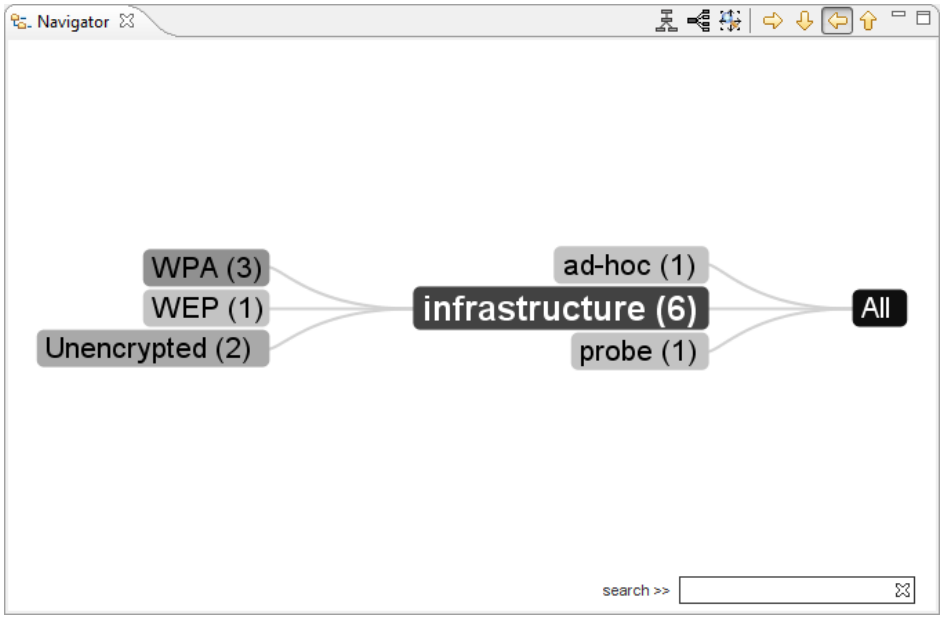
Orient Top-Bottom

This option will cause the display to show from top to bottom as shown below:



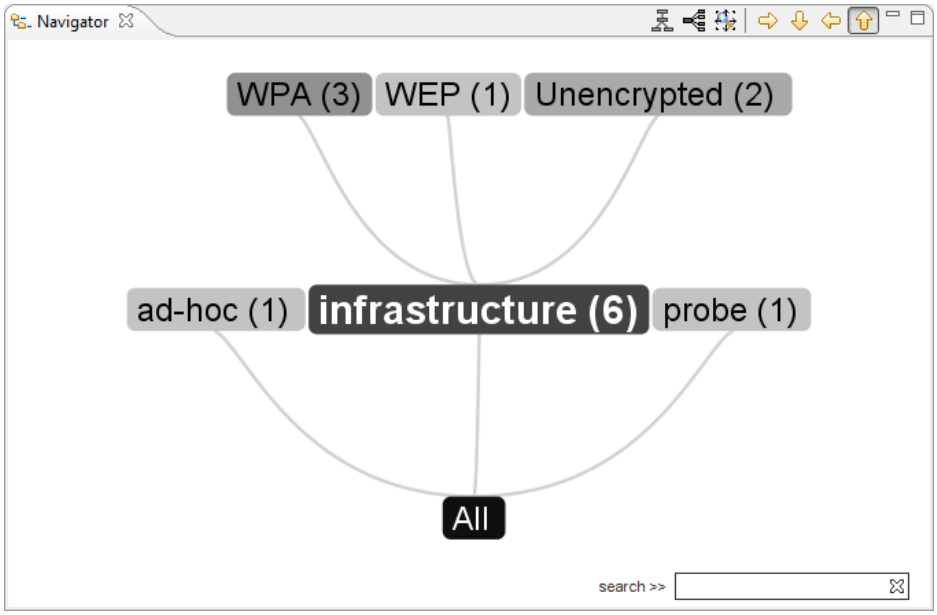
Orient Right-Left

This option will cause the display to show from top to bottom as shown below:



Orient Bottom-Top

This option will cause the display to show from top to bottom as shown below:



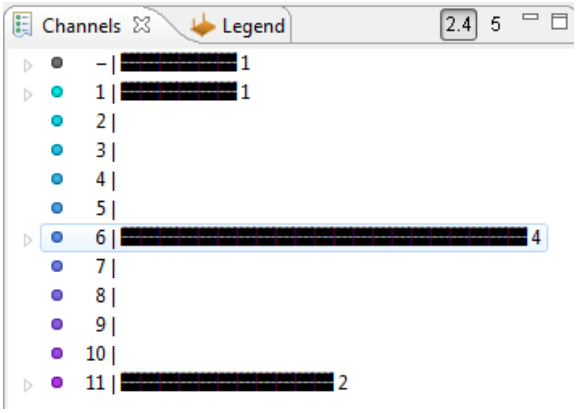
5.8 Channels View

Another beneficial feature of MeerCAT is that it can display the channel distribution of detected devices. For example, the screen below shows that Channel 6 is most widely used, which is to be expected since Channel 6 is the default channel used by most access point vendors.

1. **Expand a channel to display the individual devices operating at a channel.**

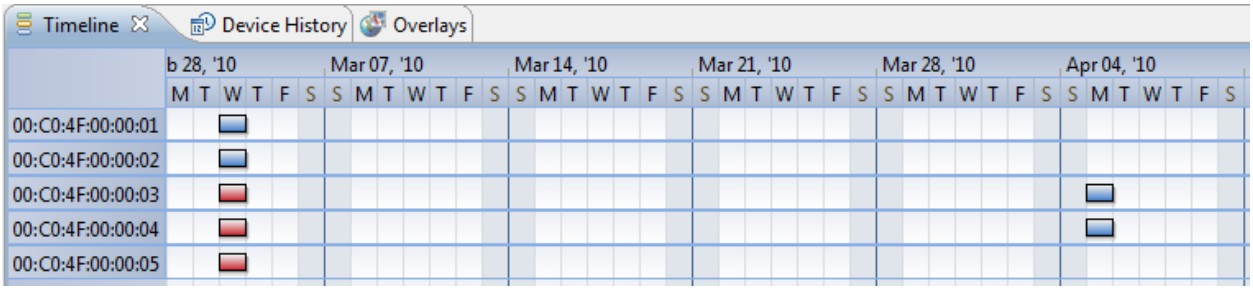
   Click on the '+' symbol adjacent to each channel to expand the view of detected devices using this channel.

   > ***Tip*** *: **Number of detected devices** operating at each channel is the number adjacent to the bar chart.*

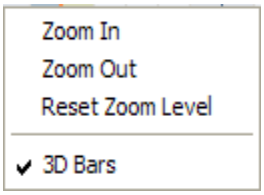


5.9 Timeline View

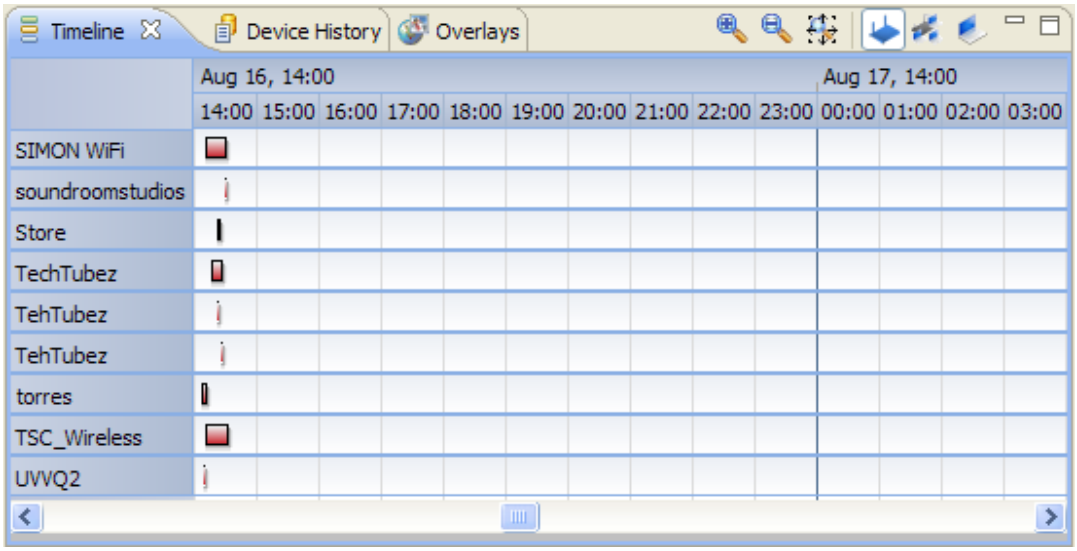
The timeline view displays data in the chronological sequence it was obtained. One can view wireless networks relative to each other on the basis of the time they were obtained. With detection runs on the same route, devices can be compared over time.


Timeline
Device History
Overlays
b 28, '10
Mar 07, '10
Mar 14, '10
Mar 21, '10
Mar 28, '10
Apr 04, '10
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S
00:C0:4F:00:00:01
00:C0:4F:00:00:02
00:C0:4F:00:00:03
00:C0:4F:00:00:04
00:C0:4F:00:00:05

A right-mouse click anywhere in the view will bring up the following menu:



Selecting Zoom In will increase the calendar scale, which can be repeated to allow hourly details to be seen. Zoom Out will shrink the calendar scale; Reset Zoom Level will return to the default view.



Toolbar

The toolbar of the Timeline view contains the following buttons:

History Mode

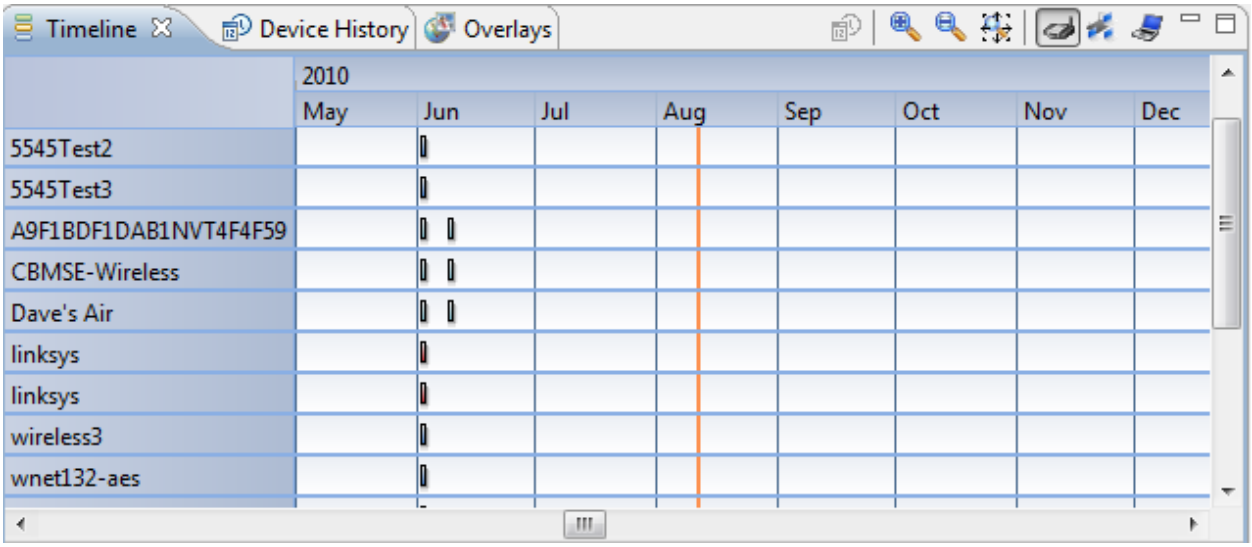
This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

Zoom In

This option will increase the calendar scale, as pictured above. Zoom In is also available using Ctrl + mouse wheel up.

Zoom Out

This option shrinks the calendar scale. Zoom Out is also available using Ctrl + mouse wheel down.

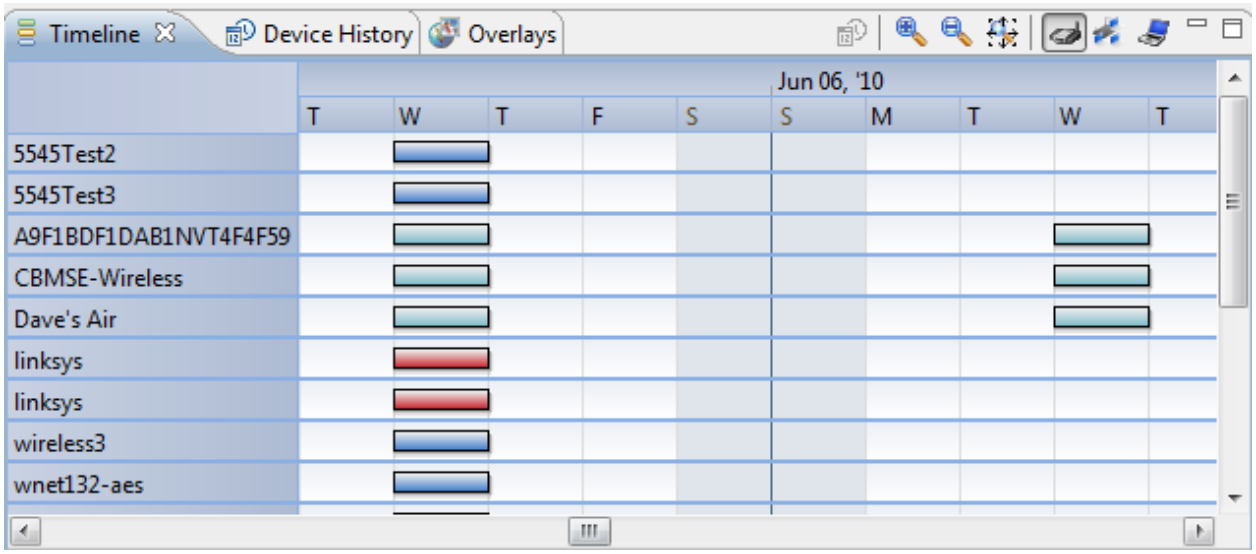


Reset Zoom

This option returns the time line to its default view.

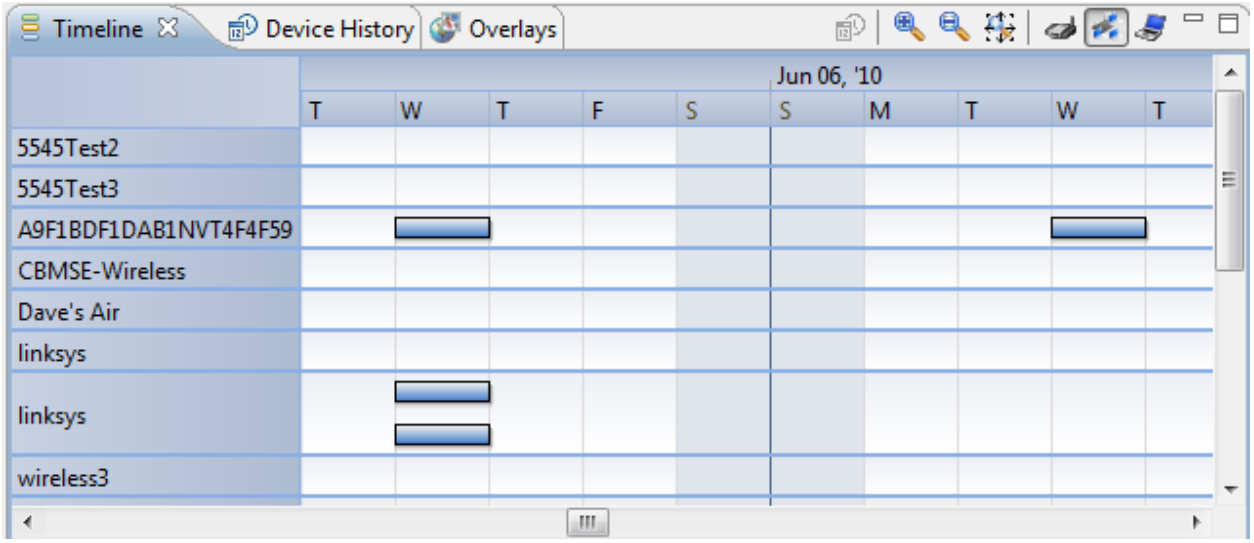
Networks

Lists all discovered network devices and shows an event indicator on dates network devices were actually detected.



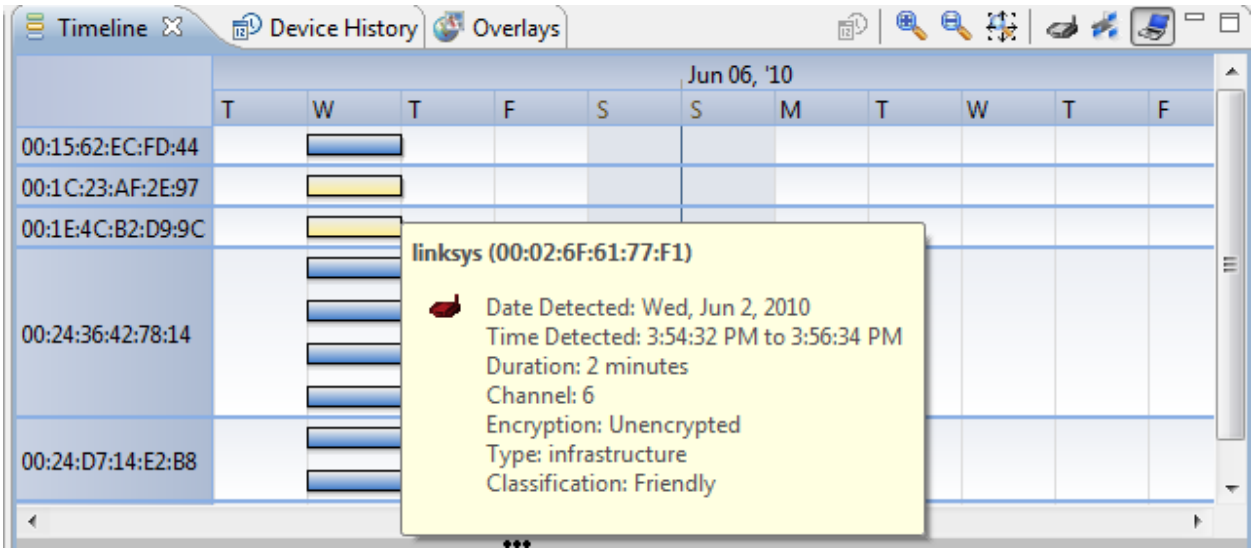
Networks with Clients

Lists all discovered network devices with an event indicator shown on dates when clients were attached to those networks. Individual event indicators are shown for individual clients. In this view, holding the mouse over an event indicator will show a pop-up window with the client details.



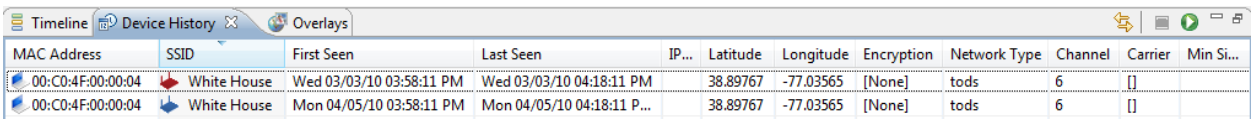
Clients and Networks

Lists all discovered clients with an event indicator on dates they connected to network devices. Holding the mouse over an event indicator will show a pop up with the individual network device details.



5.10 Device History View

This view displays data in the chronological sequence it was obtained, based on MAC address. If a device was once a network and then a client, that pattern can be seen here. You can also click the play button to animate the devices location on the 3D Geo View.



Toolbar

The toolbar of the Device History view contains the following buttons:

Link With Selection

Click on this toolbar button to activate or inactivate linking this view with device selection in other views. If not linked, device history will not change unless the Device History menu option is selected in the context menu for a device.

Stop Animation

Stops the animation in the 3D Geo view.

Start Animation

Displays an animation in the Geographic view indicating the changing location of a device over the course of the selected discovery runs.

5.11 Overlays Details

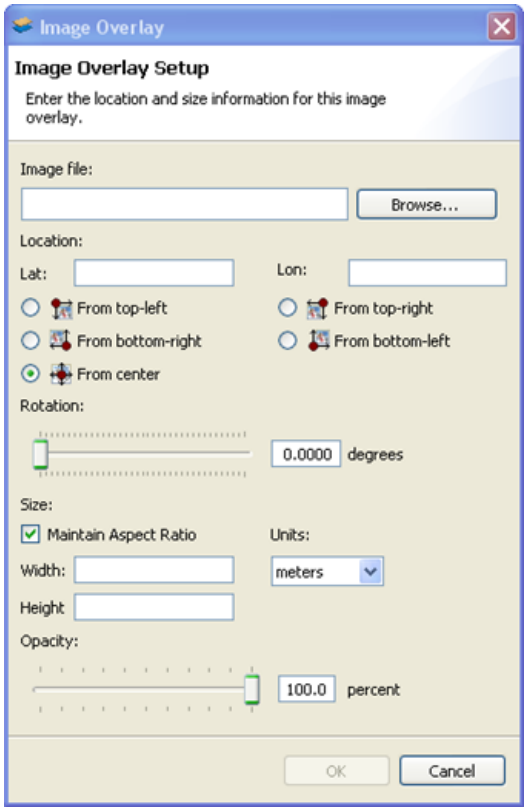
The Overlays Details View allows you to add an image such as a floor plan to the 3D Geo View. Images must be in .bmp, .gif, .jpg or .png file formats.

Toolbar

The toolbar of the Overlays view contains the following buttons:

Add Image Overlay

Opens the Image Overlay Setup window to import an image.

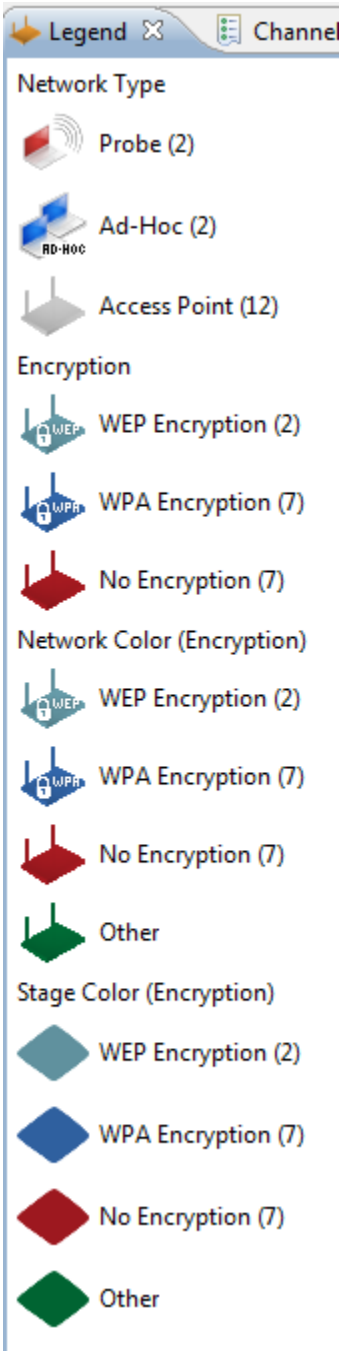


Remove Image Overlay
Removes the image overlay from the 3D Geo View.

Allow Image Dragging
Click to allow or disallow image dragging of the overlay in the 3D Geo View.

5.12 Legend View

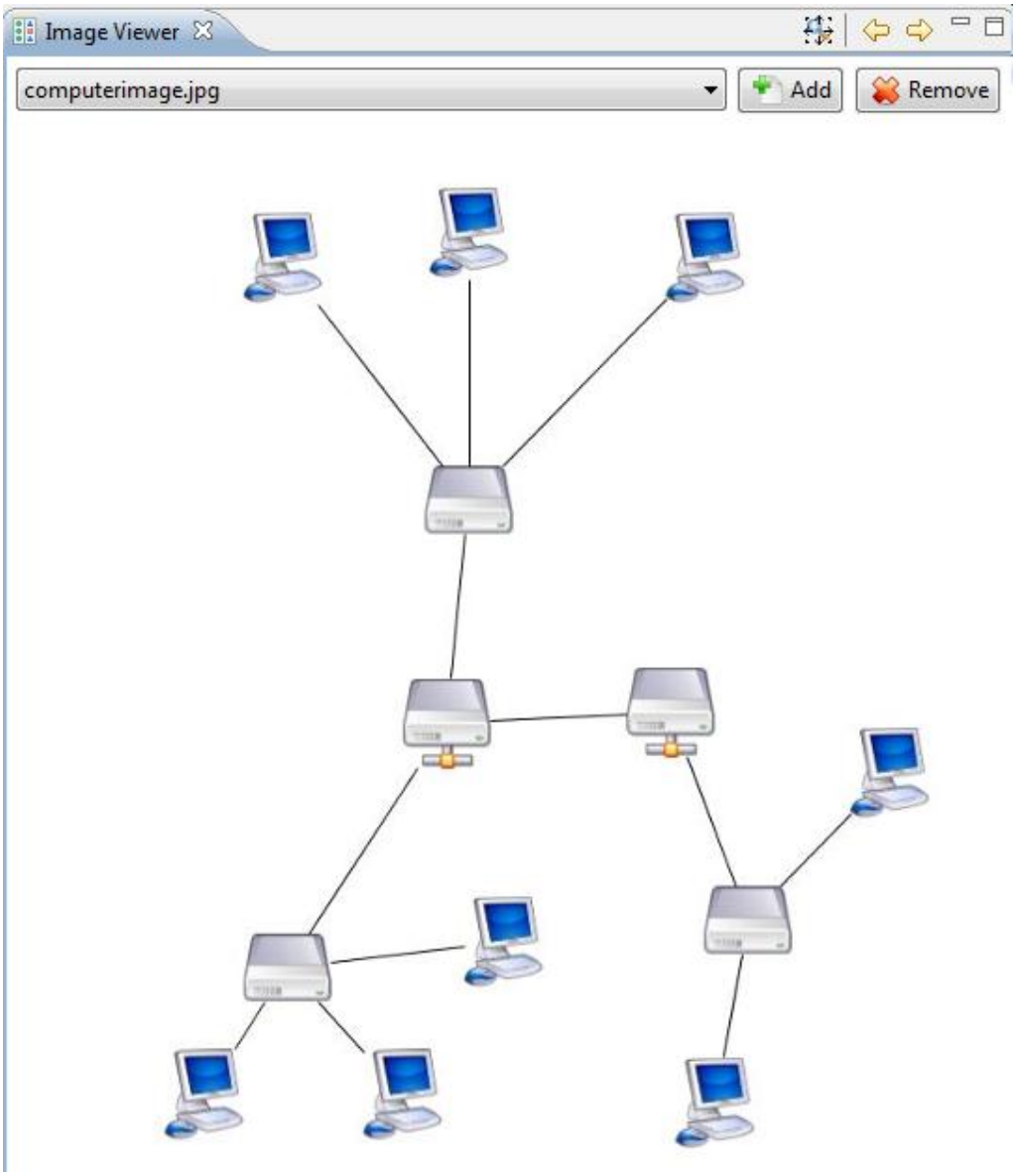
The Legend View provides quick reference to the meaning of certain visual attributes such as icons and colors within the various MeerCAT views. It allows the user to quickly see which attribute the network icons are colored by as well as which attribute the network topology "stage" is colored by. In addition, icons are provided to show the difference between Probe, Ad-Hoc, and Access Point (or infrastructure) wireless networks as they appear in the various views. The appropriate icons for encryption type are also listed. Finally, next to each entry in the legend view is a number in parenthesis (#). This number represents how many networks in the visible data set are classified by this entry.



Interaction

The legend view is automatically updated when new data becomes visible or the user changes one of the colors in the MeerCAT Preferences. In addition, double clicking on one of the icons in the legend view will bring up the preferences page that is associated with the particular attribute.

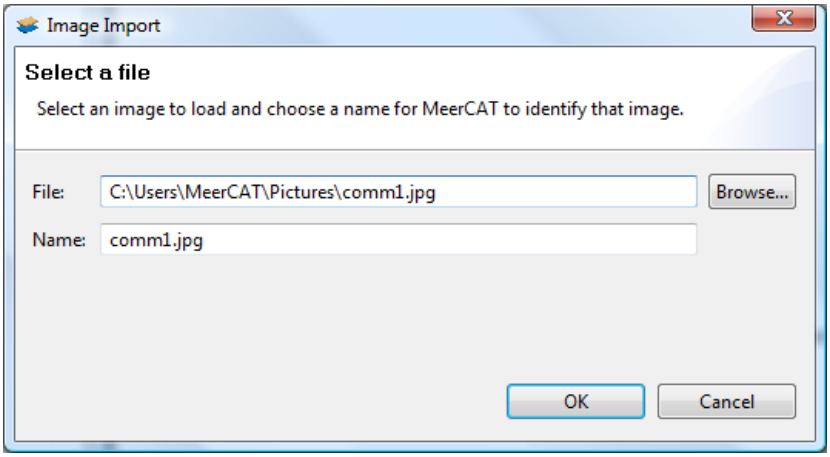
5.13 Image Viewer



Above is a screen shot of a random image being shown by the Image Viewer.

Adding Images

To add an image, click on the button at the top of the view. A dialog will appear, enter the image file's location or click the Browse… button to select a file. The PNG, GIF, JPEG, BMP, and WBMP file formats are supported by default.



Next, pick a unique Name for the image to be shown in the image list. MeerCAT will suggest a name based on the image's original file name, but be sure to pick a name that you will remember. If an image by that name already exists in the image list then a dialog will pop up asking if you would like to go back or overwrite the previous item on the image list.

Displaying Images

To display an image, simply select it from the image list at the top of the view. All images that have been successfully added will be in this list, represented by the name given during the 'add image' process.

Removing Images

To remove an image, select it in the image list and click on the

button at the top of the view. This will delete the image from the list.

User Controls

In the Image Viewer there are a number of mouse and keyboard controls that assist in the image viewing. Use the mouse wheel to zoom in and out of image. Likewise, the Page Up and Page Down keys will zoom in and out of the image, respectively. Click and hold the left mouse button anywhere in the display and move the mouse to pan the image up, down, left, or right. Likewise, the arrow keys can be used to pan the image around the display.

Toolbar

The toolbar of the Image Viewer contains the following buttons:

Zoom to Fit

This option will refit the image to fit the size of the current display.

Previous Image

This option brings up the previous image in the viewer's image list.

Next Image

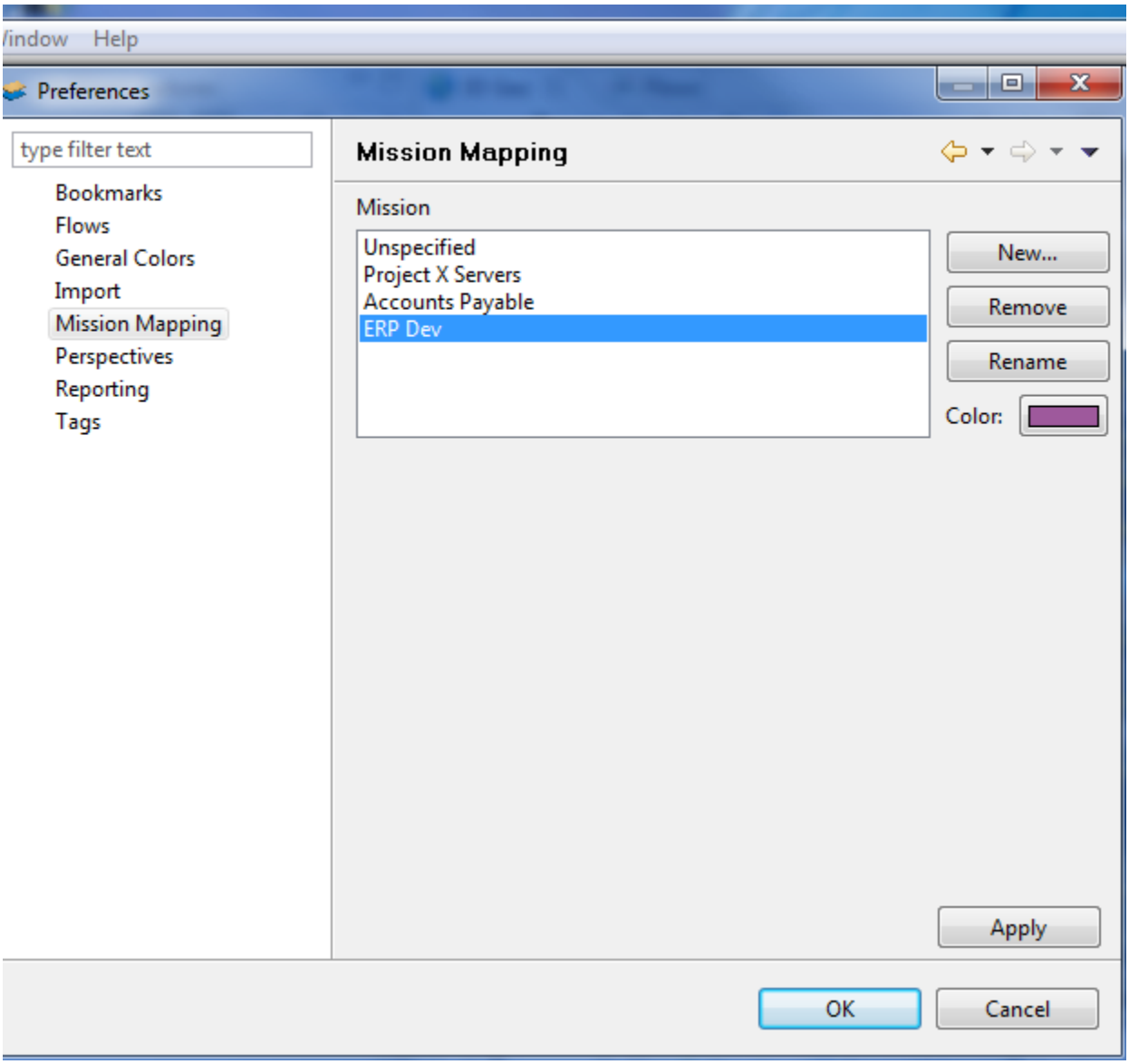
This option brings up the next image in the viewer's image list.

5.14 Mission Mapping

Mission mapping permits functional names to be added to an access point. For example, a wireless asset could have a mission of "Invoicing" or "Personnel". These access points can be grouped and colored by mission, thus facilitating visualization.

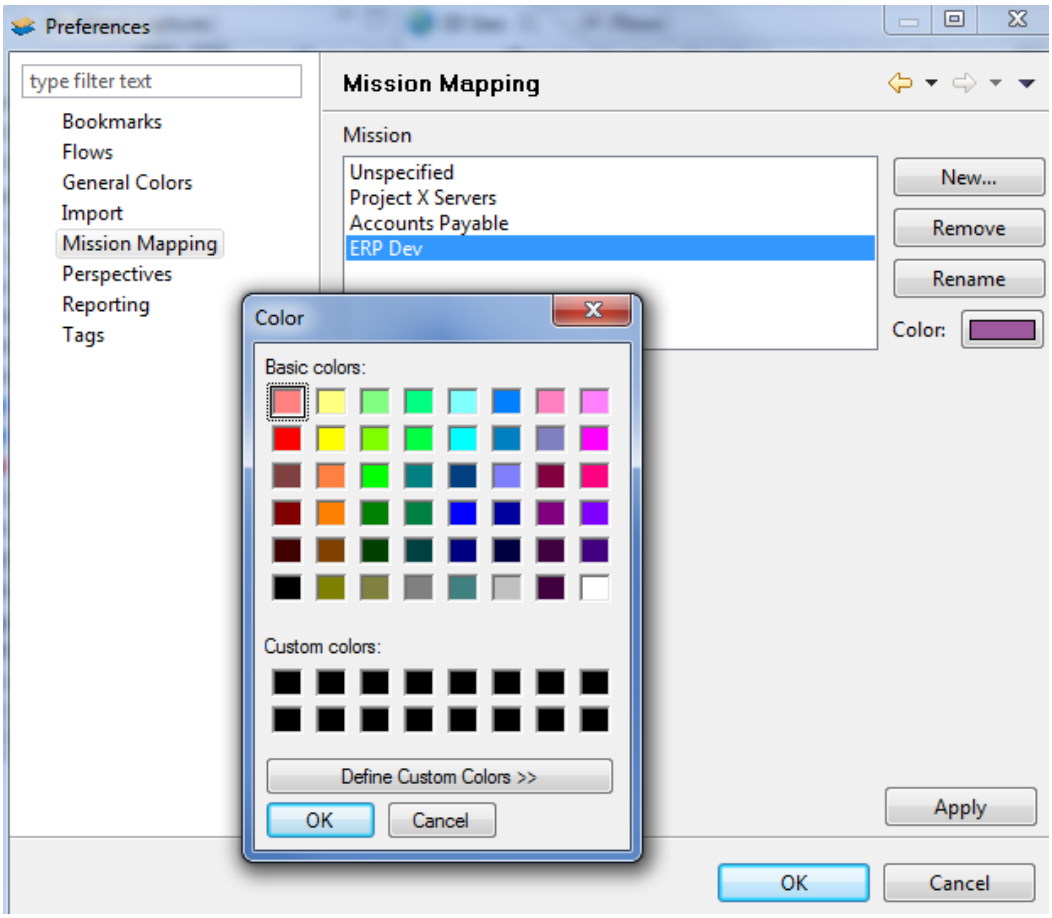
Preferences Page for Mission Mapping

Access the Mission Mapping page by Window -> Preferences. From this dialog, you can create, rename, and remove mission names, and assign colors to them. (Missions can also be added through the Device Manager – select "Other" when prompted for Mission.)



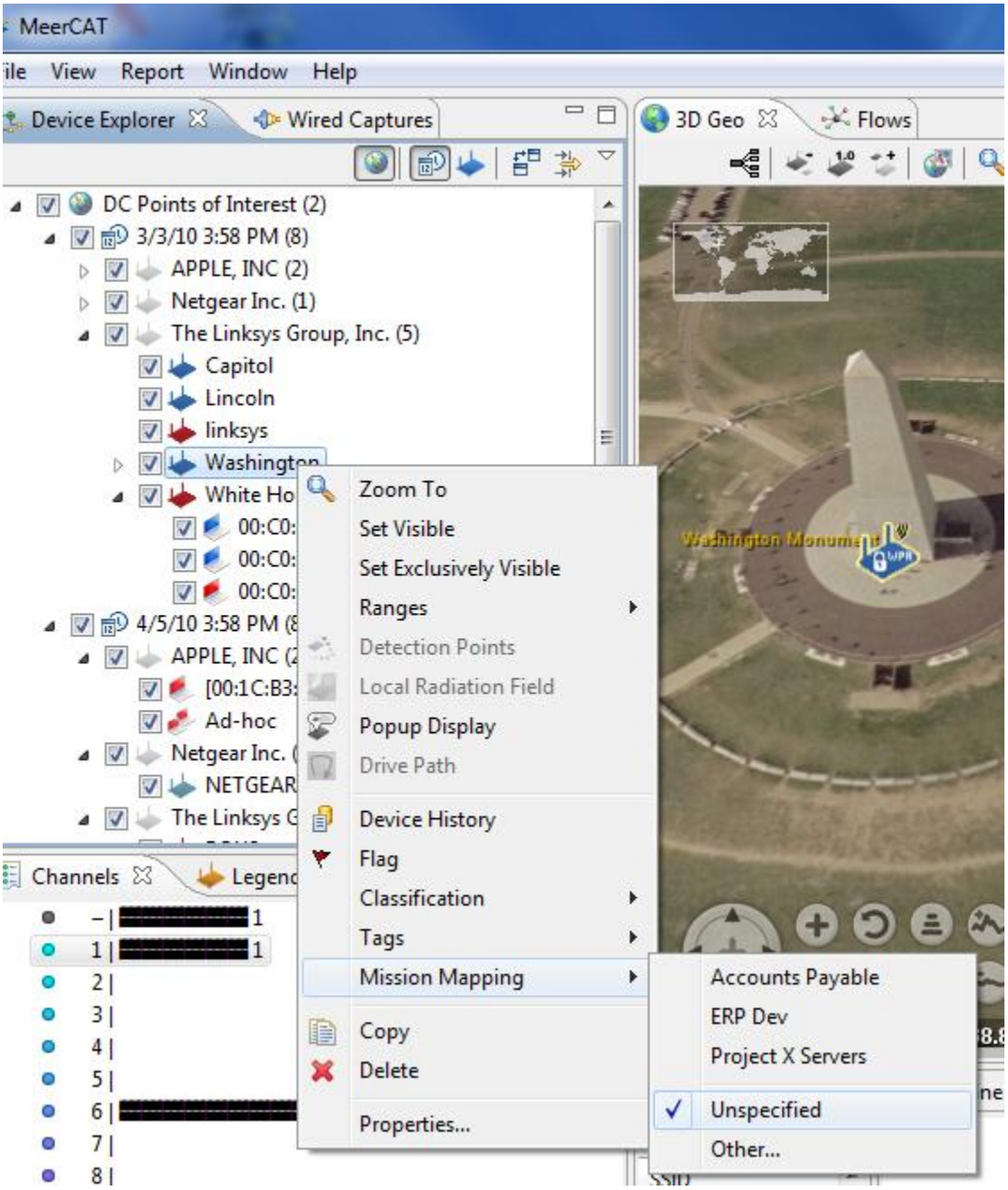
Choosing a Color for the Mission

Clicking on “Color” brings up the color picker.



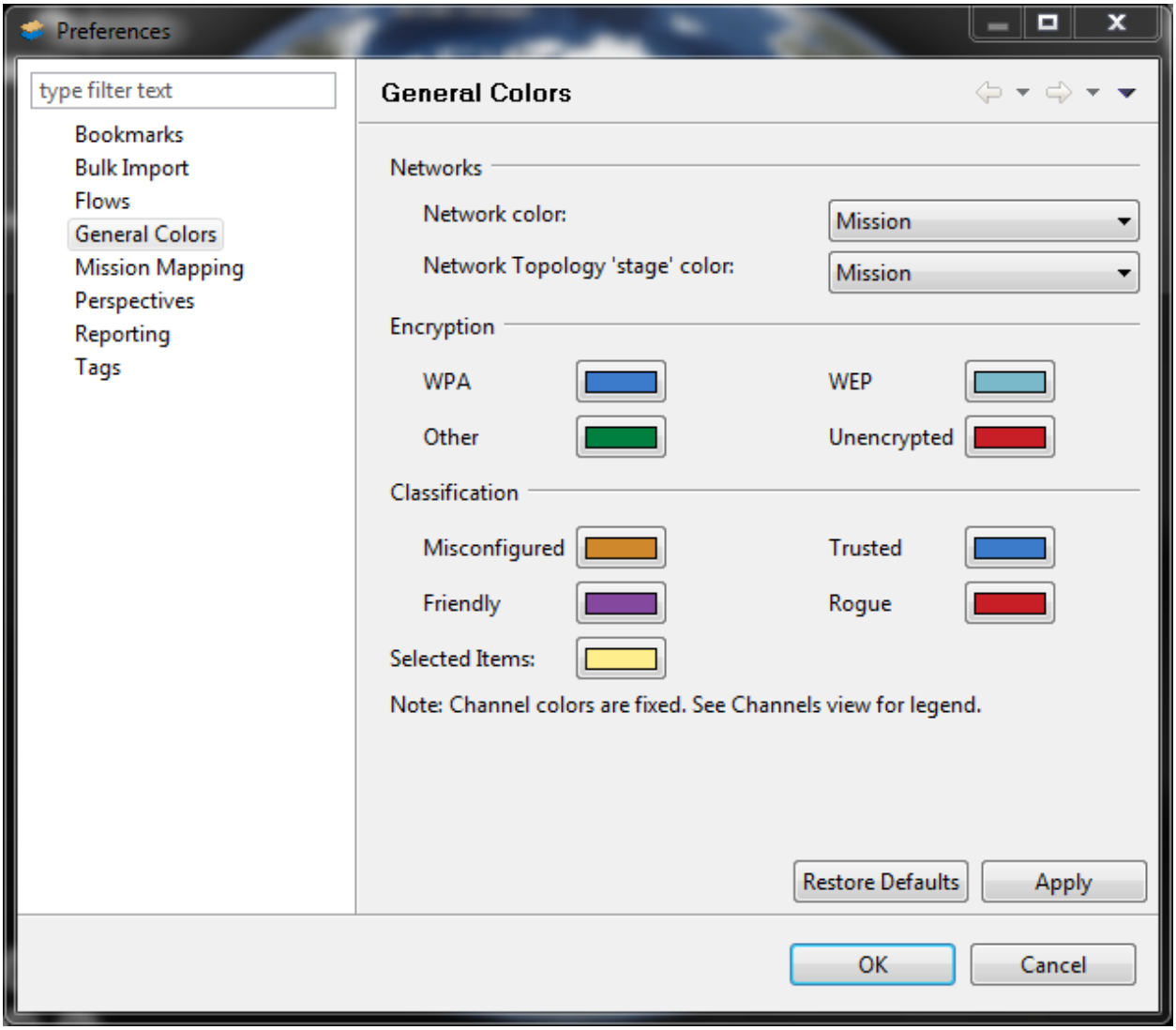
Assigning the Mission to an Access Point

Once missions are created, any access point can be assigned the mission by clicking on the choice.



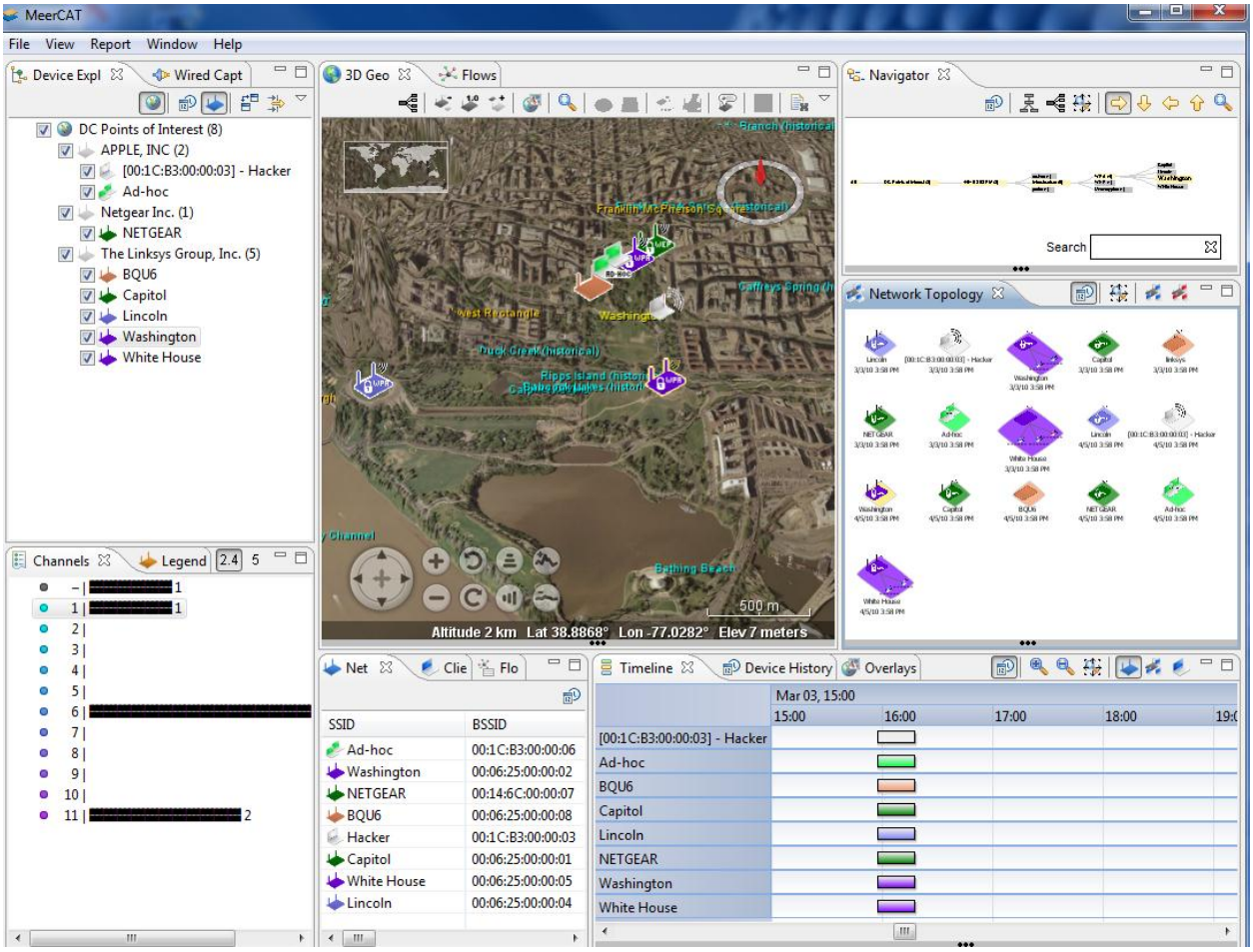
Color the Network by Mission

Access points (networks) can be colored by mission, use the Window -> Preferences again, this time selecting General Colors.



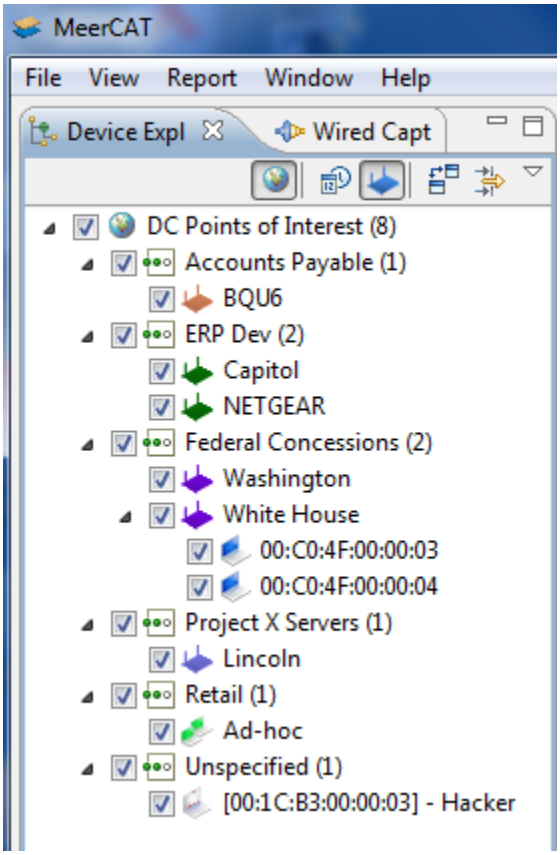
Colored by Mission

It is easy to see what function the access points have now.



Group by Mission

Access points with missions can be grouped by mission, allowing easy detection.

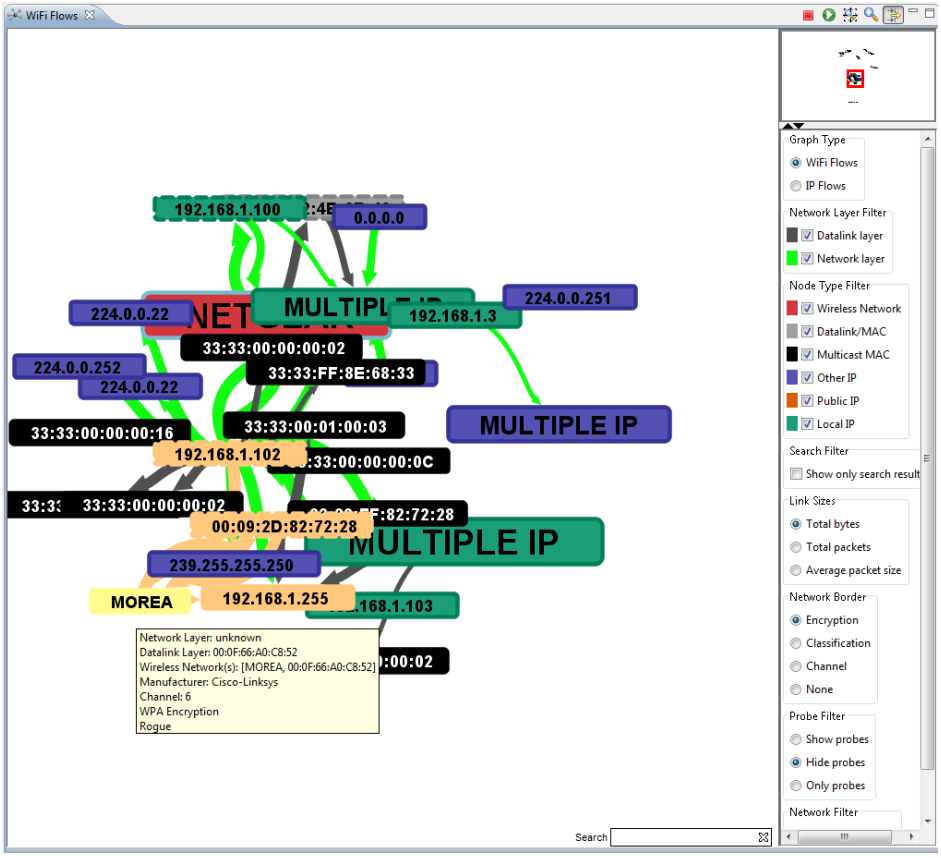


6 Communication Flow Graph

A communication flow graph is an analytical tool designed to visualize the relationships of and data flow among IEEE 802.11 wireless devices (e.g. laptops and peripherals with network cards, network access points, personal digital assistants). The flow graph is derived from processing a packet capture file. It allows users to observe data flow relationships across multiple layers of the TCP/IP and OSI network models.

6.1 Flows View

This view is a visual representation of network communication flows across multiple network layers. The nodes represent network addresses and the connections between them represent the direction, amount, and types of traffic.



Once the data is loaded, the display will lay out the graph and a small overview at the top of the filter (right) shows the entire graph as well as a red box representing the area viewable in the main display.

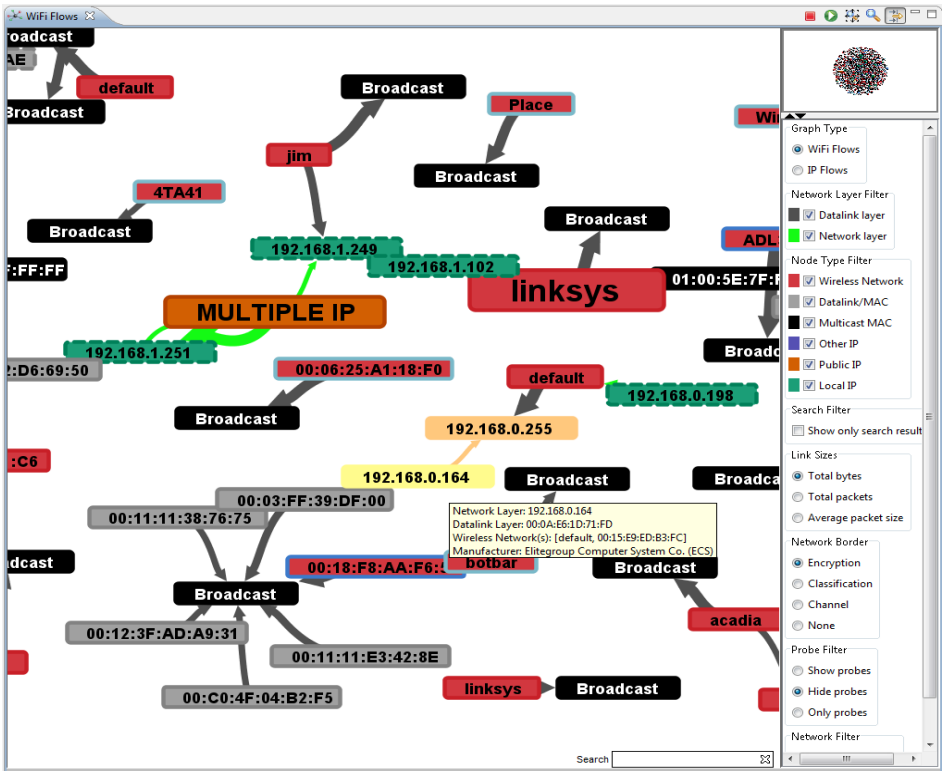
Graph Type

There are two modes in which the Flows graph can be displayed: IP Flows and WiFi Flows (default). Both graphs represent the same data set using a different method for building the actual graph. WiFi Flows uses the data link layer addresses of packet flows to distinguish between nodes and then layers any IP information on top of that. IP Flows does the opposite. That is, each node in the WiFi Flows graph belongs to a unique MAC address (there may be several Multicast MAC nodes with the same address, but only one per wireless network) but may have several IP addresses associated with it. Conversely, each node in the IP Flows view belongs to a particular IP address and may have several MAC addresses associated with it. These two modes can assist administrators in determining the ways in which different network layers act on the traffic being analyzed.

Nodes

The graph nodes each contain a label which represents a network address associated with them and they all have a fill color associated with the attributes of their communication patterns. These colors are all user manageable in the WiFi Flows area of the MeerCAT

preferences. Wireless Network nodes represent a known wireless network and are labeled with their SSID or BSSID if the SSID is not known, Multicast MAC nodes represent datalink layer broadcast and multicast addresses, and Datalink/MAC nodes represent generic datalink layer MAC addresses. These are the types of nodes that fall under the "Datalink Layer" categorization because they represent link layer hardware addresses. On the other hand, there are three classifications for nodes that exhibit network (IP) layer information. Local IP nodes are nodes that have at least one IP address in the private IPv4 range (10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255), while Other IP nodes are nodes that contain at least one multicast, broadcast, loop back, or any other reserved, non-public address. Public IP nodes represent IPv4 addresses that are public.



In WiFi Flows mode, nodes with multiple IP addresses will be depicted larger and labeled "MULTIPLE IP". In addition, Wireless Network nodes that are associated with any IP information will be depicted larger than normal nodes since their color will not be overridden by additional network layer information like their client and multicast counterparts.

A dashed border around a node shows that the node is known to be a wireless transmitter, even if not designated as a "wireless network" device. A node that is defined as a '"wireless networks" (and shown in blue by default) is known to be wireless transmitter and always has solid border with a color based on encryption or classification.

Links

The graph links represent one-way communication between two network addresses. There are color distinctions for Datalink Layer links (that is, links that exhibit Ethernet or IEEE802.11 link layer communication) and Network Layer links (links that exhibit IP communication). Their thickness is based on the amount of data passed between the devices. In addition, in the WiFi Flows mode there are symbolic connections which show the user a symbolic association between a node and one of its associated access points. If the node can be traced to the access point without adding a symbolic connection, one is not added.

Filter

The filter is composed of several parts:
Graph Type: toggles graph mode (IP Flows or WiFi Flows)
Network Layer Filter: toggles visibility of network or data link layer information. If network layer is disabled, nodes and links will revert to their data link layer attributes and label or disappear if they have none. If data link layer is disabled, any node or link without network layer information will disappear. If both are disabled, nothing is shown in the graph unless "show all networks" is selected.
Node Type Filter: toggles visual attributes and/or visibility of the various node types. A node will show visual attributes for the highest layer of information that is not filtered out.
Search Filter: when enabled, will hide any item that is not a search result or is not somehow connected to a search result in the graph.
Link Sizes Filter: toggles which attribute should be used to determine the size (thickness) of the links. The options are Total Bytes (total number of bytes in the flow represented by the link), Total Packets (total number of packets passed), and Average Packet Size (average size of packets passed through this link).
Network Border Filter: toggles which attribute should be used to determine the border color of a Wireless Network node. This can be based on the network's encryption or its device classification. It can also be disabled to show a border that is slightly darker than its fill color.
Probe Filter: allows the user to show or hide probe requests and responses. It also allows the user to show only probe requests and responses.
Show All Networks: option to force all wireless networks to be shown on the graph, even if they do not exhibit any non point-to-point communication.

User-Graph Interaction

Clicking on a node or link will globally select its associated network(s), client(s), or flow(s). Double clicking on a node will select all network, client, and flow objects associated with it or its connections. You can select multiple items by holding the SHIFT key. Likewise, when a network, client, or flow is selected globally, it will be highlighted in the display.

The search box will highlight link and nodes corresponding to a relevant MAC address, IP address, port, port name, network SSID or BSSID, and IEEE 802.11 frame types/subtypes.

Typing “www” will highlight all nodes and link with a www port associated with them. Typing “192.168.1.” will highlight all nodes and links in the 192.168.1.0/24 network.

A right click in the search panel outside of the text editing area will pop up a list of search results if there are any. The user can then click on a search result to zoom into that particular item in the graph.

For additional information on using the WiFi Flows view, see the Communication Patterns section below and the Flow Details View help section.

Toolbar

The toolbar of the WiFi Flows view contains the following buttons:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

Stop Layout

This option stops the force directed layout from acting on the graph.

Run Layout

This option will run the force directed layout for the length of time specified in the WiFi Flows preferences.

Zoom to Fit

This option will refit the display to fit the size of the current display.

Magnifier

This option will turn the magnifier on or off. The magnifier will make nodes within the “glass” around the mouse point appear larger. Use the mouse wheel to determine the level to which the nodes are enlarged. Hold the CTRL key and use the mouse wheel to change the range (size of the glass) around the mouse point that the magnification should affect.

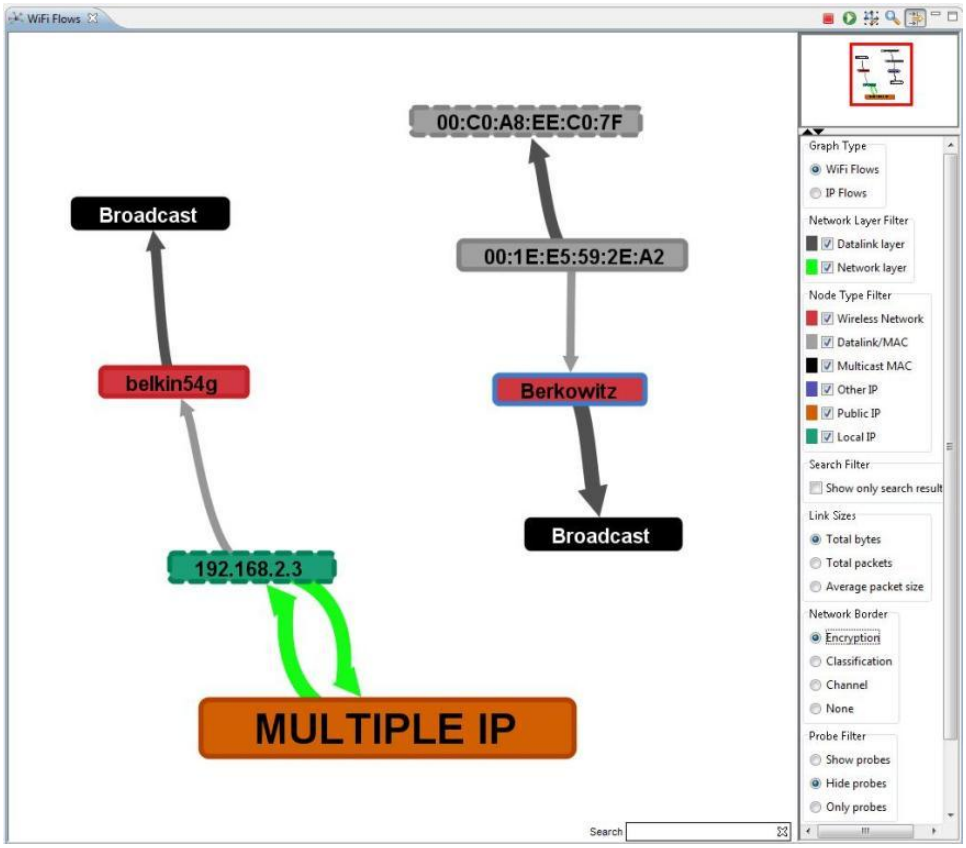
Toggle Filter

This option will hide or show the WiFi flows filter.

Communication Patterns Usage Scenario

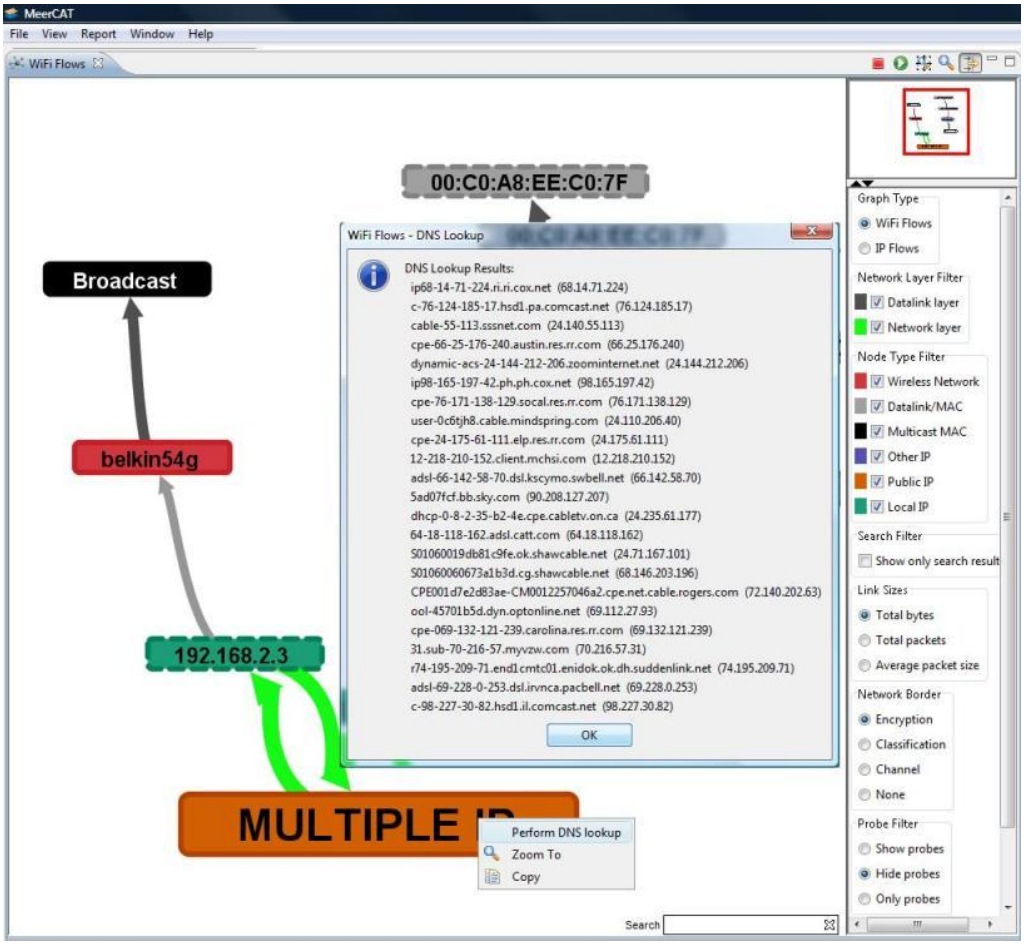
The WiFi Flows View is a useful tool in analyzing wireless network flows. This help section contains examples on how to use the WiFi Flows View to learn more about the structure and vulnerability of wireless networks. For a general approach to understanding the WiFi

Flows view, please see the WiFi Flows help in the Using MeerCAT - Fundamental Tools section.

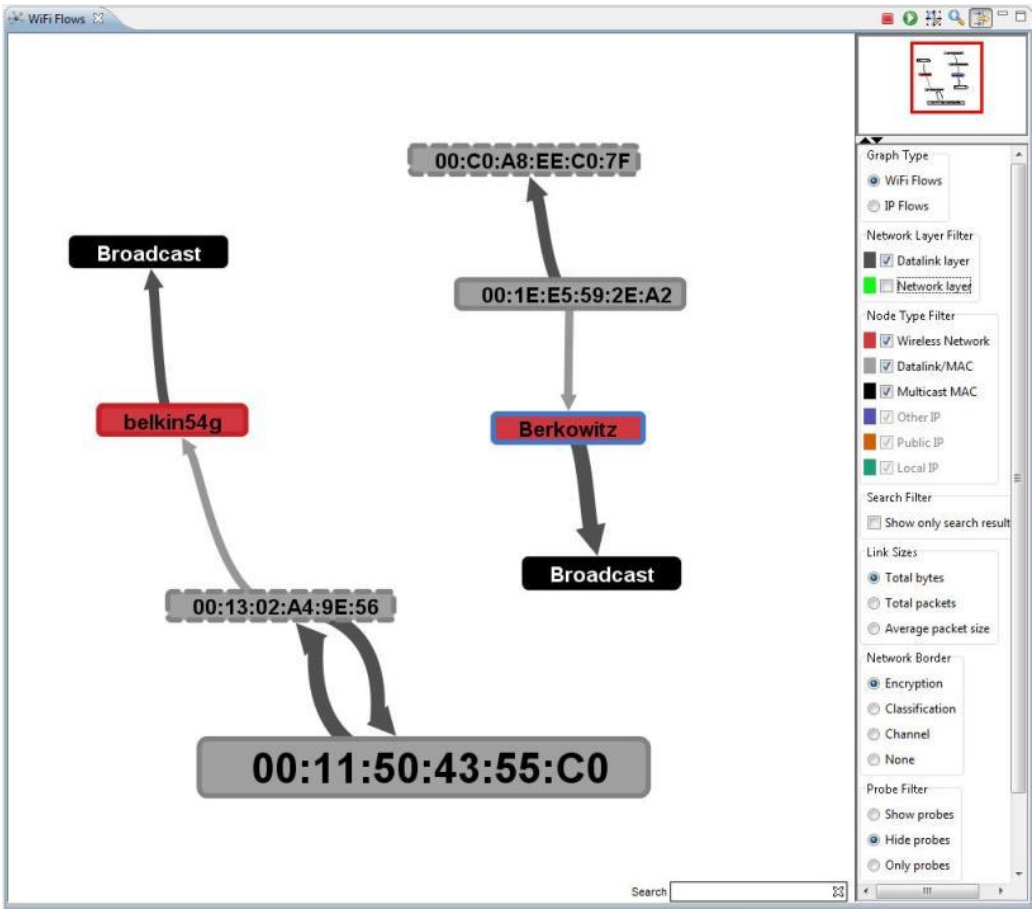


Above is a picture depicting two wireless access points: Berkowitz and belkin54g. Since the border filter is set to "encryption" this means that Berkowitz is using an encryption standard that is not WEP or WPA and belkin54g is using no encryption. These color classifications are available in the legend view and can be edited in the MeerCAT preferences. What's important to note here is that the two of these wireless networks are set up and behave very similarly except for their encryption, which makes a world of difference in wireless networking.

A good indication of whether or not a node belongs to a wireless interface is to look at its border. If it has a dashed border, then the available packet data shows sufficient evidence to suggest that the particular address belongs to a wireless transmitter. That makes the 192.168.2.3 and 00:C0:A8:EE:C0:7F nodes known wireless assets, probably somebody's laptop.



In this second screen shot, we have decided to go straight to the large node labeled "MULTIPLE IP" in the belkin54g network. In addition to this link layer address being the owner or next hop of multiple IP addresses, they are also remote IP addresses that we are concerned with. To begin, we right click on the node and perform a DNS lookup. This gives us an idea as to what sort of IP addresses belong to this link layer entity.



Using the "Network Layer" filter we told the WiFi Flows graph to ignore network layer information when displaying the visual attributes of the nodes. As a result, we are shown the MAC address of each of these nodes. The important thing that we discover is that the large node's MAC address is very close to that of the belkin54g BSSID, 00:11:50:43:55:C1. This suggests that it is probably an Ethernet interface on the wireless access point while 00:11:50:43:55:C1 is the MAC address belonging to the wireless interface. A similar thing is going on with the 00:1E:E5:59:2E:A2 node of the Berkowitz network, suggesting the same thing is going on there.

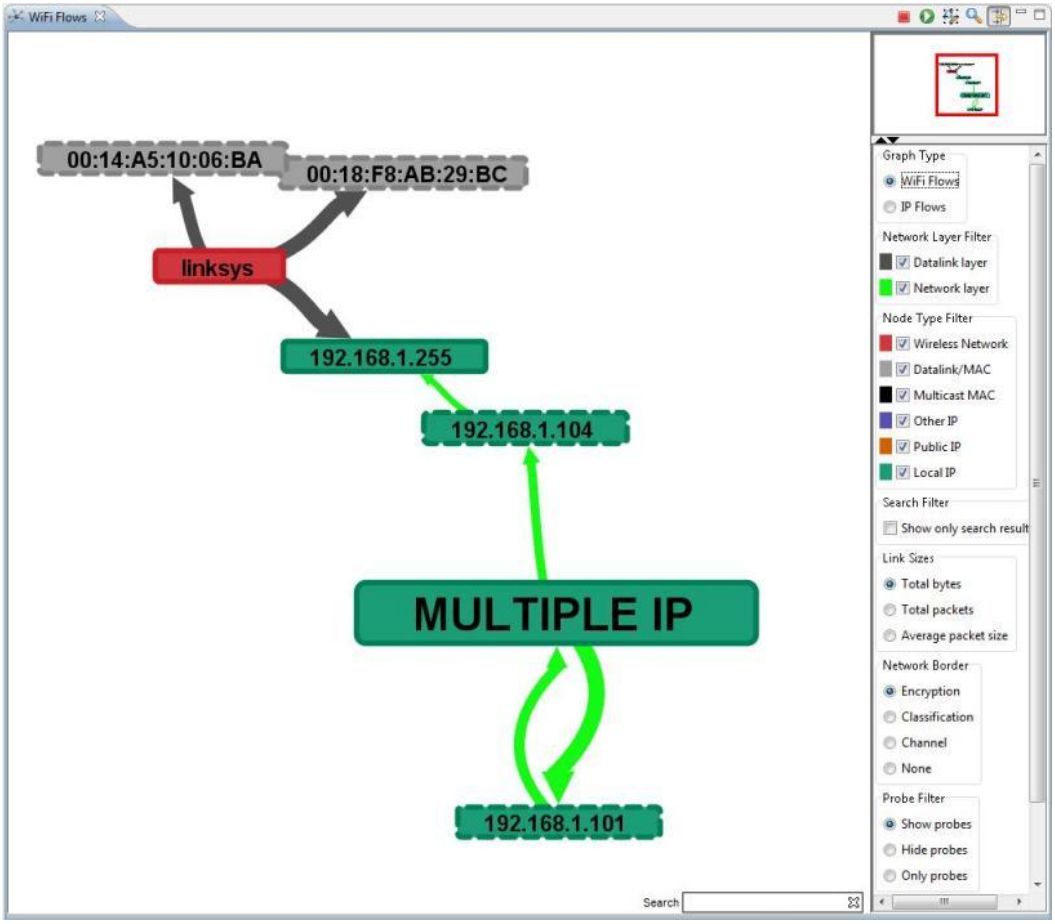
The belkin54g example is a very common signature for someone who plugged a wireless access point into an active switch port and started using it with "out of the box" open configuration. This is a problem for a network security officer, because anybody listening to the radio signals nearby can see any connections and information being passed by the network's client(s). Unless you have decrypted the packet files ahead of time with software such as Wireshark (http://www.wireshark.org), seeing IP layer communication in this view should draw an immediate red flag.

Analyzing part of the edge tooltip between the MULTIPLE IP node and 192.168.2.3 as well as the DNS results shows that the local wireless client on belkin54g is connected to many

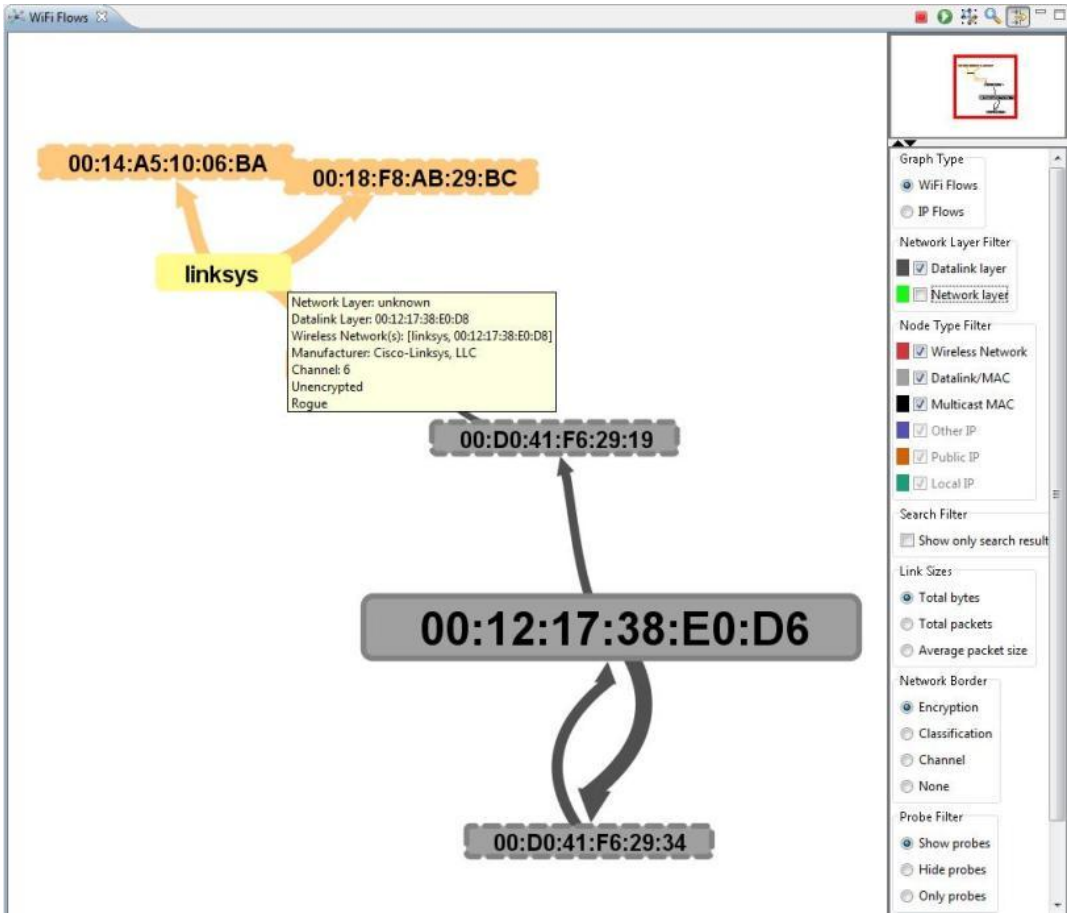
home broadband computers on various unreserved ports, possibly indicating that the access point is being used as a gateway for an Internet gamer.

In the Berkowitz network, we cannot see any IP layer information because the packets are encrypted. As such, we cannot determine how many or what kind of computers 00:C0:A8:EE:C0:7F is talking to if 00:1E:E5:59:2E:A2 is a routing interface. This is ideal for a network administrator, because the only thing that is being broadcast is that there is traffic passing between the access point and one of its clients.

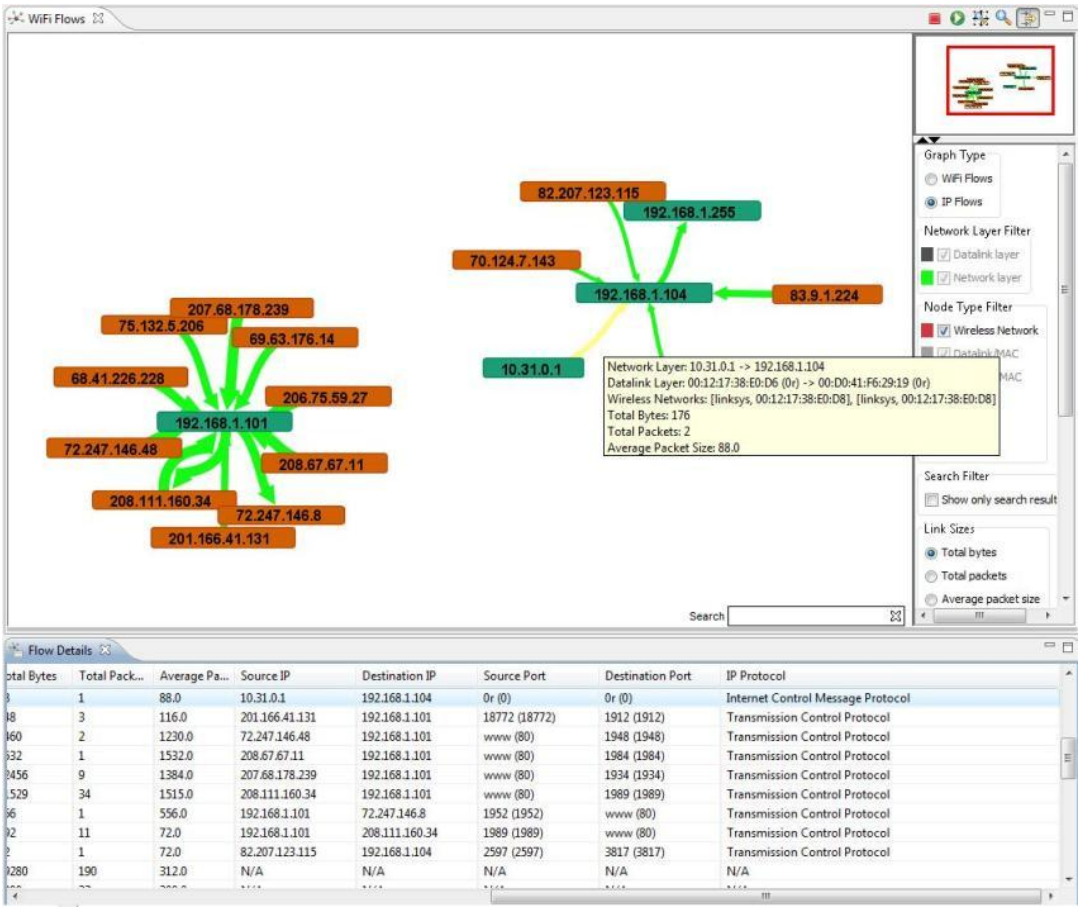
WiFi LAN Example



In the example above, we see two wireless clients, 192.168.1.104 and 192.168.1.101, communicating with a local node 192.168.1.255 (probably broadcast, which we will find out soon) and another “MULTIPLE IP” node that is labeled local.



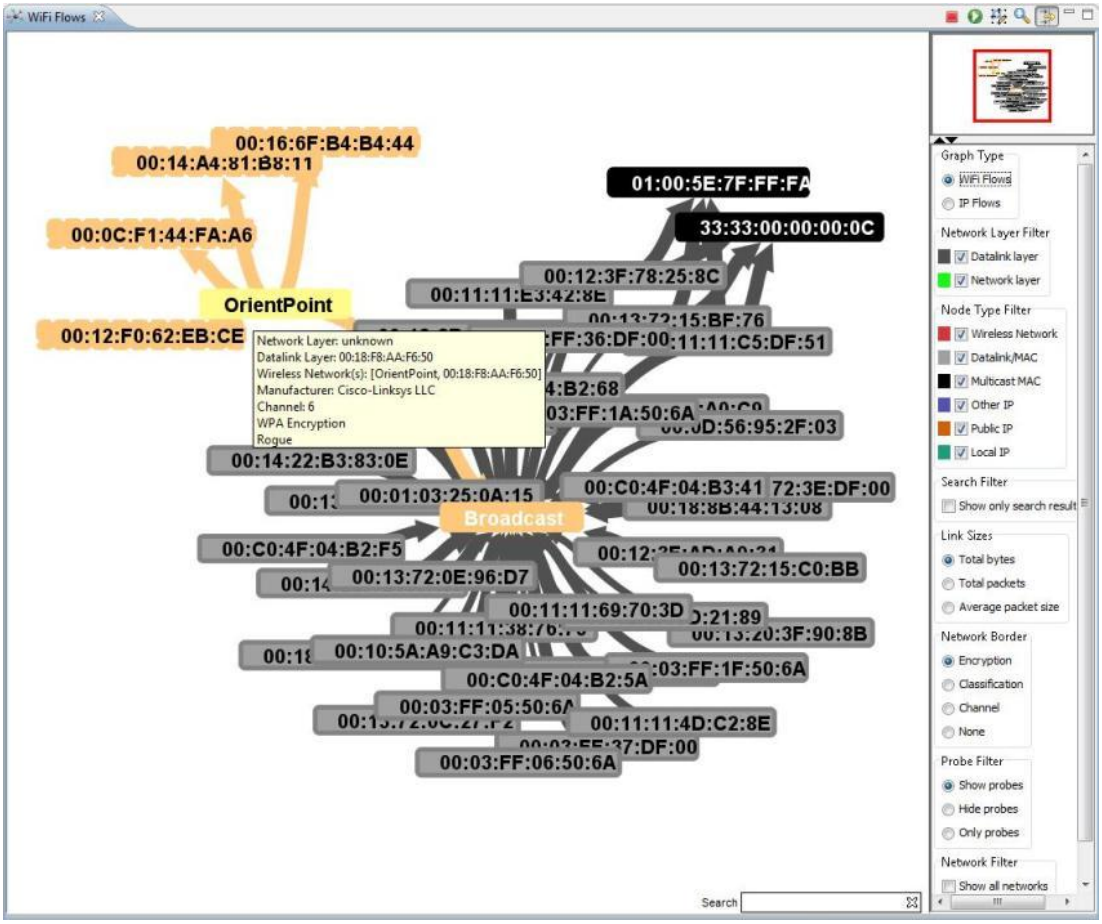
Above, we have disabled the network layer information of the graph and can see the similarities between the BSSID of the linksys access point and the MAC address of the local IP node associated with multiple IP addresses in our capture. Again, this suggests that the latter is the interface to which traffic is sent that will pass over a wired network.



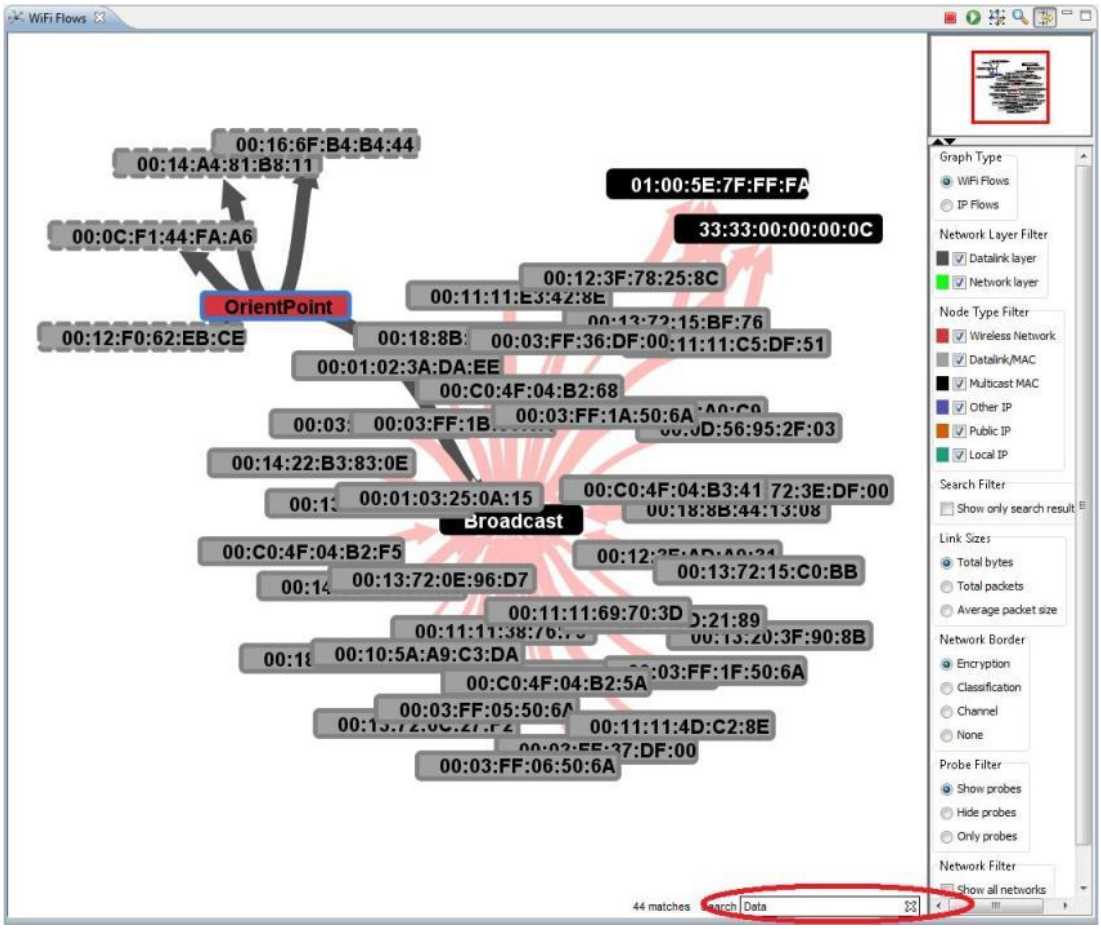
Since we are observing IP communication and there are several IP addresses aggregated into the single node, we switch the graph type over to IP Flows mode. This mode builds the graph nodes based on IP address, giving us a flow graph similar if not the same to other network layer flow graphs.

In this view, with the help of the flow details table, we can see that information is being passed from the IP address 10.31.0.1 to 192.168.1.104 via port 0 in an Internet Control Message Protocol (ICMP) packet. If 10.31.0.1 happens to belong to a router interface on the LAN to which the linksys access point is connected to, which is probably the case, we can identify that not only is the unencrypted linksys access point a back door to the LAN but also that a potentially vital network asset's IP address is being exposed through unencrypted radio broadcast.

WiFi Broadcast Domain Example



In this example, we see the access point OrientPoint talking to its broadcast MAC address. In addition, there are several other generic data link layer nodes that are also sending broadcast messages through the air. Since it looks like there's over 30 nodes sending broadcast messages to the air through the access point this should draw a red flag, if not for security issues but for performance since large broadcast domains can cripple network performance.



In trying to figure out what's going on here, we can run a quick search for Data frames. IEEE 802.11 frames contain a type and subtype field which describes what kind of frame is being transmitted. There are three major types: Data, Management, and Control and each one has a number of subtypes associated with it. It turns out that all of these nodes are broadcasting data (rather than beacon frames for example which don't always imply a connection) so it's safe to assume that all of these nodes lie in the same broadcast domain.

A more important thing to notice here is that none of these data link layer MAC addresses can be considered wireless transmitters since there were no frames intercepted that would suggest that they have this capability. This is visualized by the network border, and only nodes with a dashed border can be affirmed as wireless transmitting devices. Upon further analysis of the network topology (trying to figure out what devices belong to what MAC address), we found that the reality of this graph is that most if not all of the data link layer clients are actually machines on the same wired LAN segment as the access point. This is just not good practice, if not for performance then for security as well considering all broadcast traffic from the wired LAN is being transmitted in the air as well, not only exposing the MAC addresses of several assets on the wired network but also providing a steady flow of data through the air which could be used to aid a hacker in exploiting encryption key vulnerabilities that exist in protocols such as WEP.

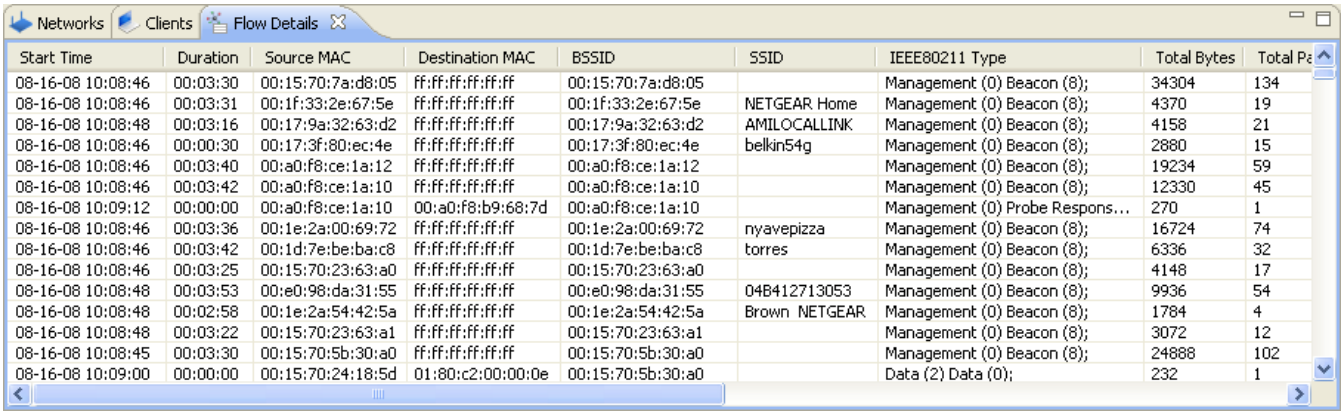
One possible fix to this is to put the access point on a different VLAN or subnet than the other clients, allowing a router to take care of passing any traffic that might need to be passed between the wired and wireless segments of the LAN rather than just automatically forwarding the broadcasts.

6.2 Flow Details

The Flow Details View is a companion to the Flows View, and requires that packet data was captured during the detection run and loaded into MeerCAT. This view allows the users to see detailed information about a particular packet capture. It can also be sorted by any one of the data fields.

This table view is tied in with selecting wireless networks and clients in other views, which will allow analysts to quickly associate traffic with individual networks.

- IEEE 802.11 and Ethernet frame details are shown for all intercepted packets that are encapsulated in one of these link layer frames.
- IP and ARP flows also show detailed information about network and transport (TCP/IP) layer attributes of a communication flow such as source and destination ports, addresses, and protocols.



Start Time	Duration	Source MAC	Destination MAC	BSSID	SSID	IEEE80211 Type	Total Bytes	Total Pa
08-16-08 10:08:46	00:03:30	00:15:70:7a:d8:05	ff:ff:ff:ff:ff:ff	00:15:70:7a:d8:05		Management (0) Beacon (8);	34304	134
08-16-08 10:08:46	00:03:31	00:1f:33:2e:67:5e	ff:ff:ff:ff:ff:ff	00:1f:33:2e:67:5e	NETGEAR Home	Management (0) Beacon (8);	4370	19
08-16-08 10:08:48	00:03:16	00:17:9a:32:63:d2	ff:ff:ff:ff:ff:ff	00:17:9a:32:63:d2	AMILOCALLINK	Management (0) Beacon (8);	4158	21
08-16-08 10:08:46	00:00:30	00:17:3f:80:ec:4e	ff:ff:ff:ff:ff:ff	00:17:3f:80:ec:4e	belkin54g	Management (0) Beacon (8);	2880	15
08-16-08 10:08:46	00:03:40	00:a0:f8:ce:1a:12	ff:ff:ff:ff:ff:ff	00:a0:f8:ce:1a:12		Management (0) Beacon (8);	19234	59
08-16-08 10:08:46	00:03:42	00:a0:f8:ce:1a:10	ff:ff:ff:ff:ff:ff	00:a0:f8:ce:1a:10		Management (0) Beacon (8);	12330	45
08-16-08 10:09:12	00:00:00	00:a0:f8:ce:1a:10	00:a0:f8:b9:68:7d	00:a0:f8:ce:1a:10		Management (0) Probe Respons...	270	1
08-16-08 10:08:46	00:03:36	00:1e:2a:00:69:72	ff:ff:ff:ff:ff:ff	00:1e:2a:00:69:72	nyavepizza	Management (0) Beacon (8);	16724	74
08-16-08 10:08:46	00:03:42	00:1d:7e:be:ba:c8	ff:ff:ff:ff:ff:ff	00:1d:7e:be:ba:c8	torres	Management (0) Beacon (8);	6336	32
08-16-08 10:08:46	00:03:25	00:15:70:23:63:a0	ff:ff:ff:ff:ff:ff	00:15:70:23:63:a0		Management (0) Beacon (8);	4148	17
08-16-08 10:08:48	00:03:53	00:e0:98:da:31:55	ff:ff:ff:ff:ff:ff	00:e0:98:da:31:55	04B412713053	Management (0) Beacon (8);	9936	54
08-16-08 10:08:48	00:02:58	00:1e:2a:54:42:5a	ff:ff:ff:ff:ff:ff	00:1e:2a:54:42:5a	Brown_NETGEAR	Management (0) Beacon (8);	1784	4
08-16-08 10:08:48	00:03:22	00:15:70:23:63:a1	ff:ff:ff:ff:ff:ff	00:15:70:23:63:a1		Management (0) Beacon (8);	3072	12
08-16-08 10:08:45	00:03:30	00:15:70:5b:30:a0	ff:ff:ff:ff:ff:ff	00:15:70:5b:30:a0		Management (0) Beacon (8);	24888	102
08-16-08 10:09:00	00:00:00	00:15:70:24:18:5d	01:80:c2:00:00:0e	00:15:70:5b:30:a0		Data (2) Data (0);	232	1

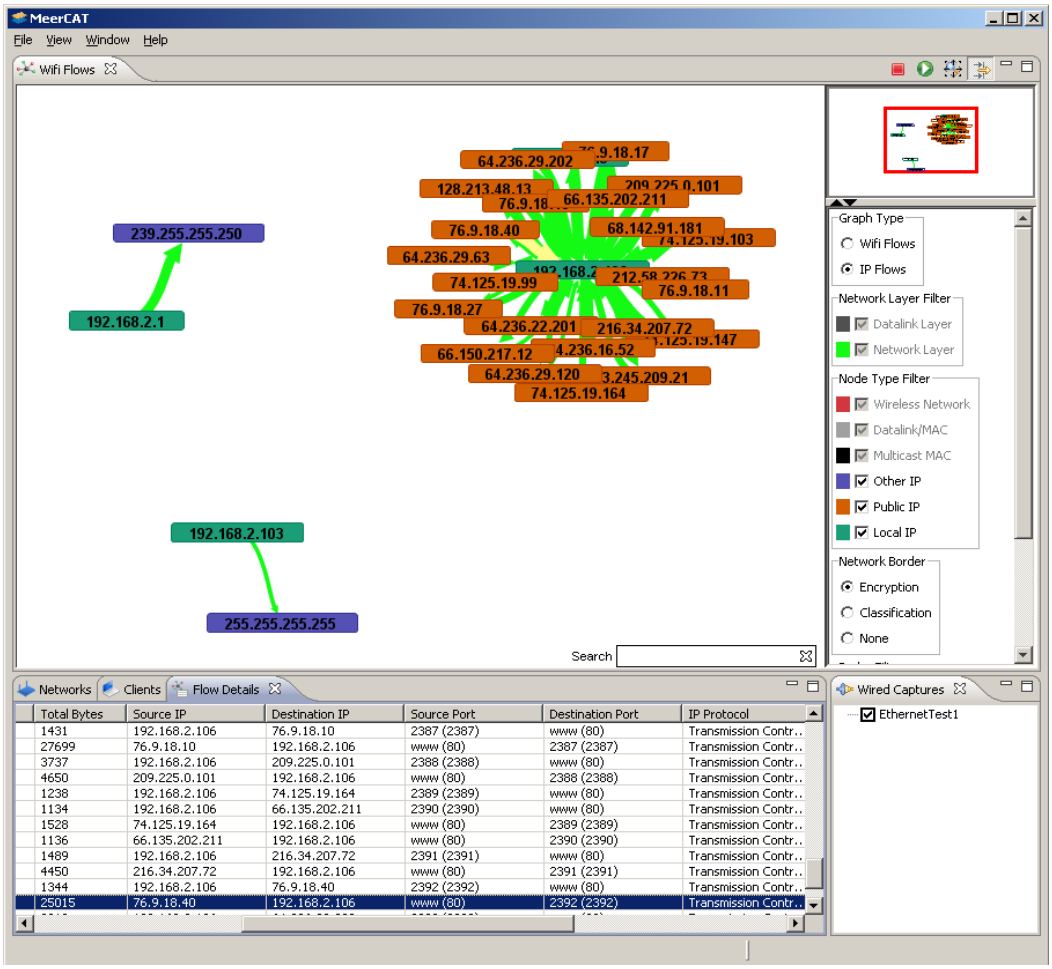
Toolbar

The toolbar of the Flow Details View contains the following buttons:

History Mode

This option is only available when the Device Explorer is in Network Mode. If enabled, this view will be populated with data from every historical instance of this wireless network in the current database. If it is not enabled, the view will be populated with only the latest historical instance of the particular network(s) unless a network is selected in the Device History view, in which case the view will be updated to show only the selected instance of the particular network.

6.3 Wired Captures



Above is an example of the three views that wired capture data has an effect on in MeerCAT.

Wired Captures View

In the Wired Captures view, each wired capture that was imported is listed and may also be removed by right clicking on the capture and selecting “Delete.” Checking off the capture will make the capture data visible to any view that will handle it.

Flows View

In the Flows view, wired capture data is only considered when the graph is in IP Flows mode. For more information on the Flows View, see the Flows View help section.

Flow Details View

In the Flow Details view, wired data is displayed just like wireless data, except the BSSID and SSID fields will be blank for each of these flows as there are no associated wireless networks.

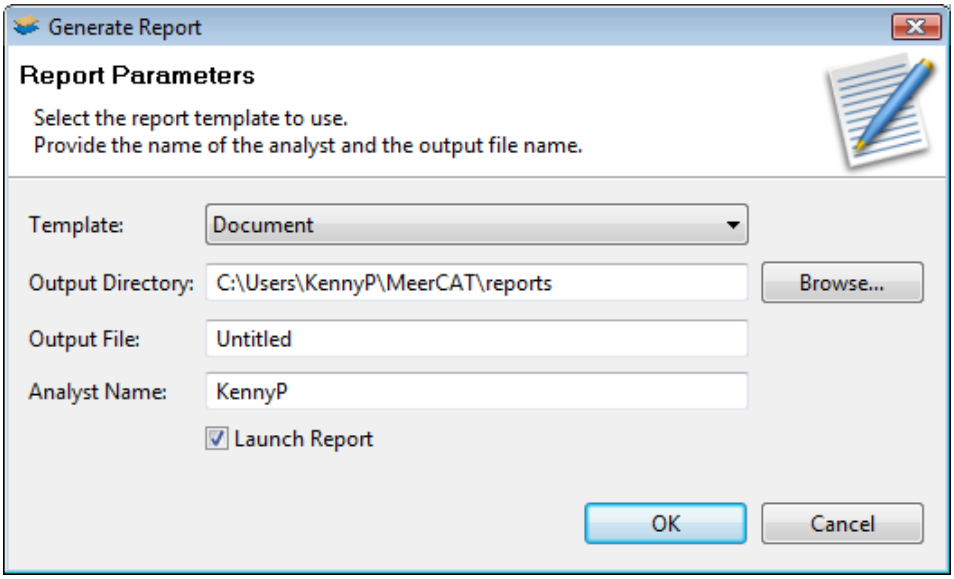
7 Reporting

7.1 Reporting Features

MeerCAT contains various ways to report and present the results of an audit or security analysis. This includes copy to clipboard, exporting a view to an image file, drag and drop views to other applications, e-mail views, and template based report generation to Word or PowerPoint Most of these features are available via the main Report menu. Annotations can also be added to views, which are then included in the report and also in e-mail reports.

Generate Report

The Report -> Generate Report menu will take a given Word or PowerPoint template and insert associated views and view annotations. MeerCAT comes with two default templates, one for Word and one for PowerPoint. If a view is not visible, it will not be added to the report.



Options:

Template - Select from available Word or PowerPoint templates. . Only the Word reports can contain detail table lists for Networks, Clients, Device History, and Flow Details. If custom templates have been created, they will also appear here.

Output Directory - Browse to the location where you would like the report to be saved to. The default directory can be changed in the Reporting Preferences options in Window -> Preferences.

Output File - The filename to be used when saving the report.

Analyst Name - Name to be inserted into the report template when generating report. The default analyst name can be changed in the Reporting Preferences options in Window -> Preferences.

Launch Report - If this is checked, the report will automatically open after being generated. This will use whatever is currently configured to be your default WorldML or PowerPoint viewer.

Copy Screenshot of Active View

This menu option will copy the active view to your systems clipboard. This can be useful if you simply want to paste the view to another application. Ctlr+Shift+C is the shortcut key for this operation.

Save Screenshot of Active View

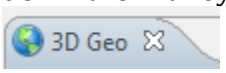
This menu option will export the active view to an image file. Available image types are PNG, JPEG, GIF, and Bitmap. Ctrl+Shift+S is the shortcut key for this operation.

Email Screenshot of Active View

This menu option will create a new email message using your default mail client (e.g. Outlook). This message will include the active view as an image attachment and a view's annotation will be used for the body of the email message. Ctrl+Shift+E is the shortcut key for this operation.

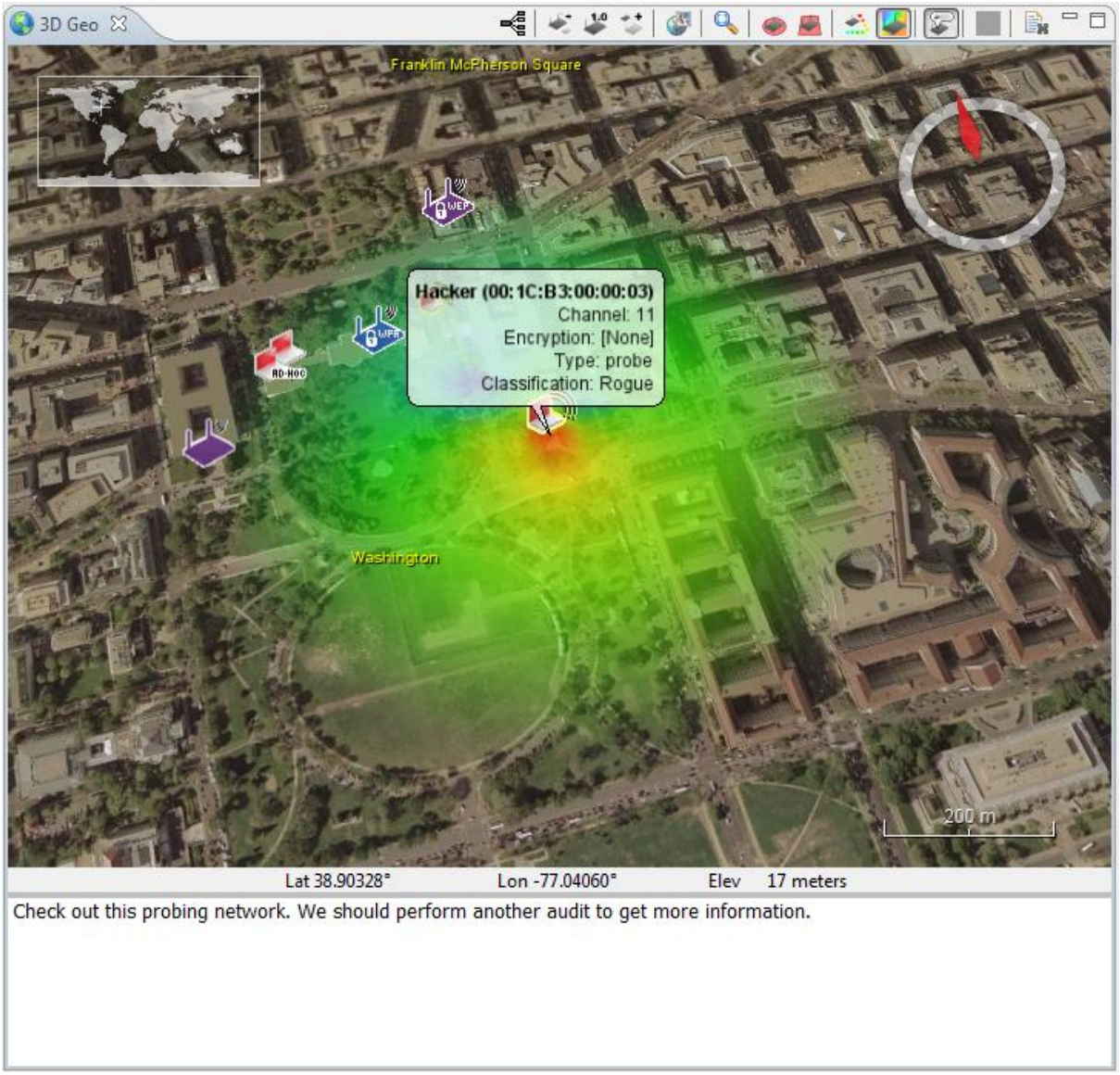
Drag and Drop

Each view can be dragged and dropped into other applications. This can be done by holding down the Alt key while dragging a views title as shown here:



View Annotations

Annotations can be added to the 3D Geo, Flows, Network Topology, Navigator, and Timeline views, similar to notes in PowerPoint. To show the view annotations, double-click or drag the gray bar at the bottom of each view. This will expand the view annotations control. Here you can type in notes, which will be including in Word, PowerPoint, and email report.



7.2 Report Templates

MeerCAT comes with two default templates, one for Word and one for PowerPoint. These templates can be modified using Word, PowerPoint, or OpenOffice, or a new template can be created and used within MeerCAT. Templates are stored and configured in the reportConfig folder, located in your user home MeerCAT folder. On Windows XP this is usually located at C:\Documents and Settings\<username>\MeerCAT and on Vista it is located at C:\Users\<username>\MeerCAT. To have a new template appear within MeerCAT, you must add the template to the reports.xml file in the reportConfig folder.

Images

Image views can be added to a report template by dragging and dropping the associated view's JPG file in the reportConfig folder. The position can be placed anywhere within the document or presentation. Only the width of the image is maintained when the report is generated. The height will maintain the aspect ratio based on the width.

Tables

Table views, including the Networks, Client, Flow Details, and Device History tables, can be added to a report using the following keyword text. This text will be replaced at report generation time with the actual table data.

- MeerCAT.Networks
- MeerCAT.Client
- MeerCAT.DeviceHistory
- MeerCAT.FlowDetails

Annotations

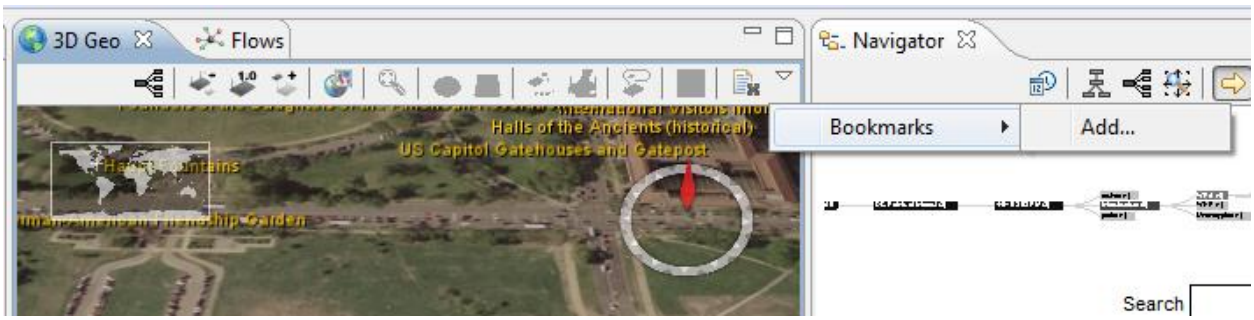
View annotations can be added to a document or presentation. The following keywords are used:

- MeerCAT.Geo3D.Notes
- MeerCAT.Flows.Notes
- MeerCAT.NetworkTopology.Notes
- MeerCAT.Navigator.Notes
- MeerCAT.Timeline.Notes
- MeerCAT.ImageViewer.Notes

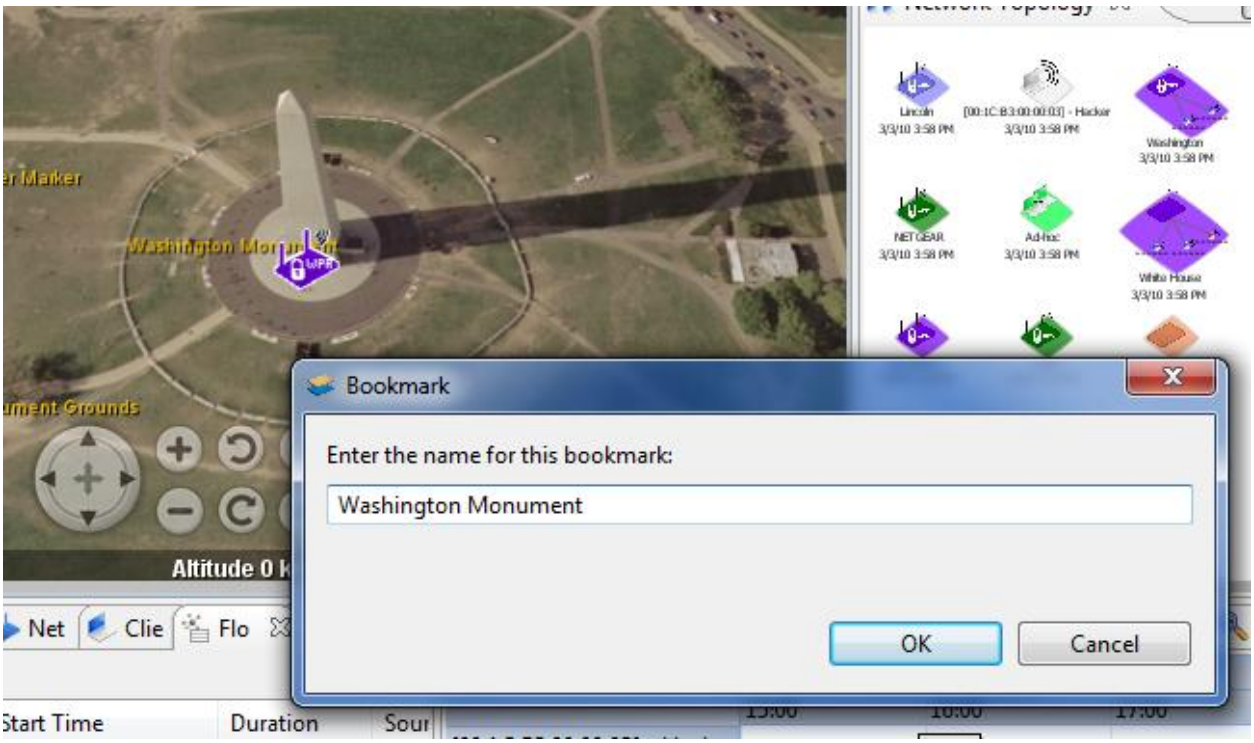
8 Other Preference Options

8.1 Bookmarks

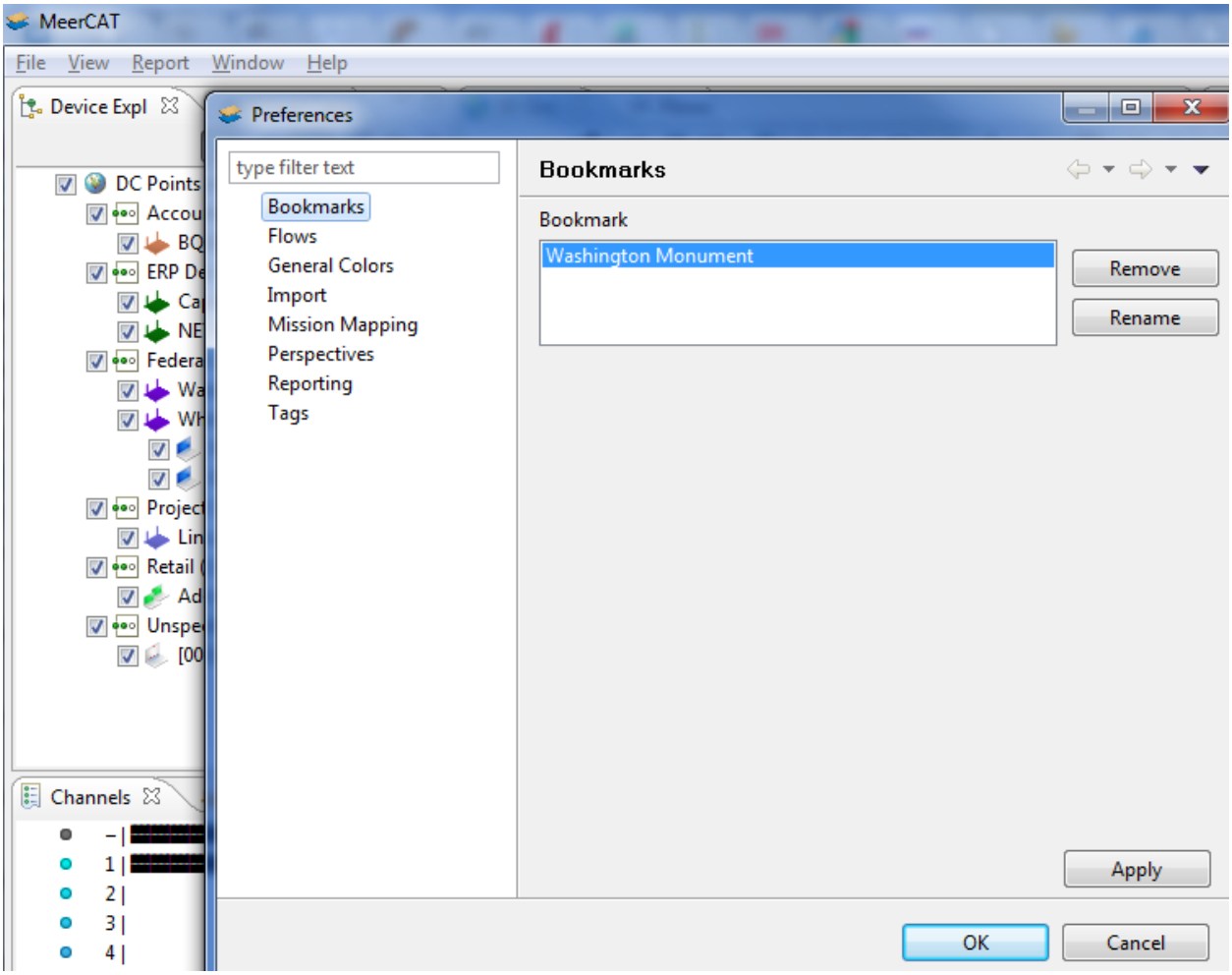
Bookmarks can be used to save the settings in a particular 3D Geo View, such as zoom level or specific areas of interest. Select the **View Menu** from the 3D Geo Toolbar. Then choose **Bookmark -> Add.**



Next enter a memorable name for the bookmark, then click OK.

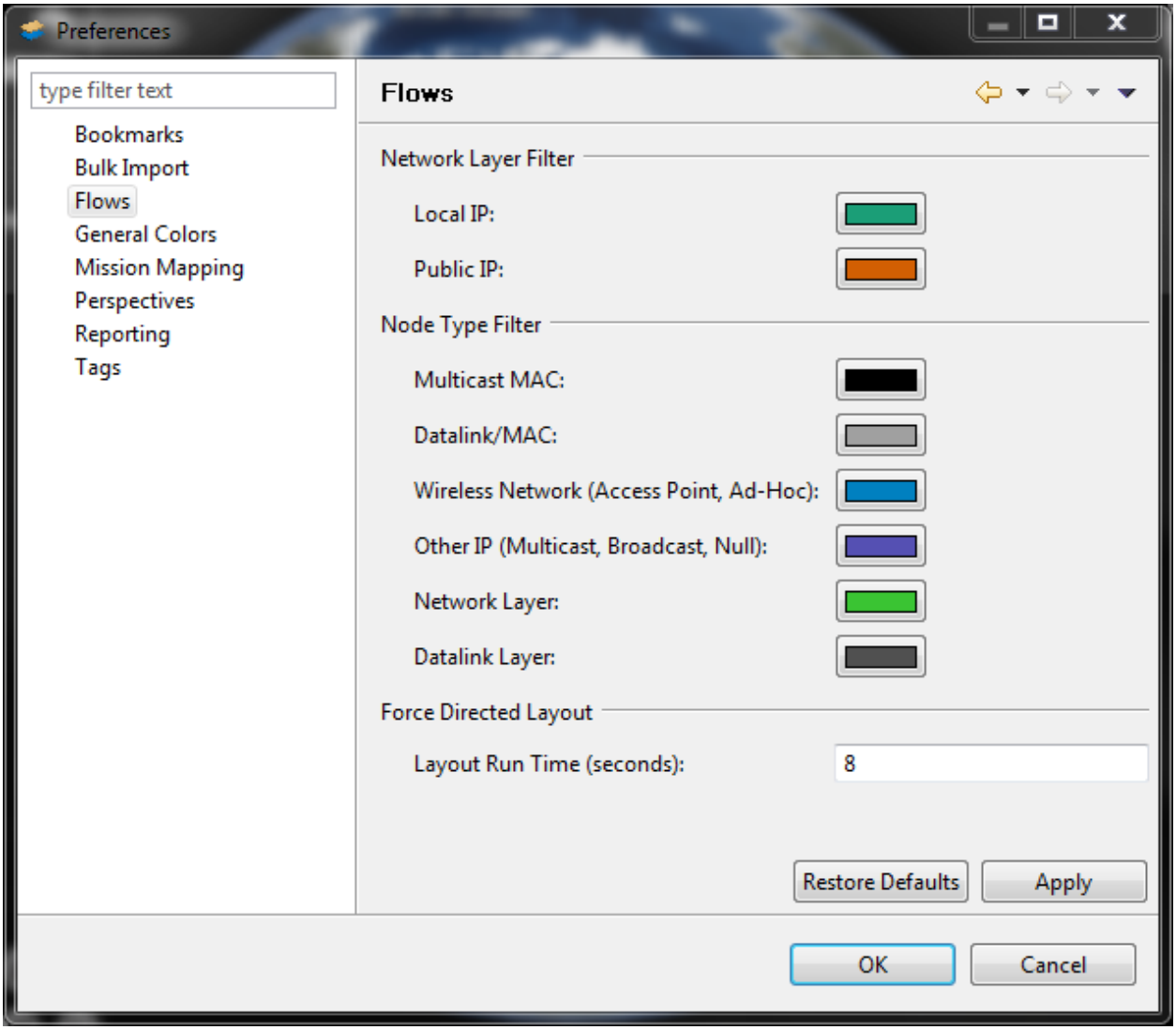


Bookmarks can be deleted or renamed through the Preferences menu. From the MeerCAT main menu, select **Window -> Preferences**. Then click on **Bookmarks** to see this dialog box. Highlight the bookmark of interest, then select **Remove** or **Rename** to maintain bookmarks.

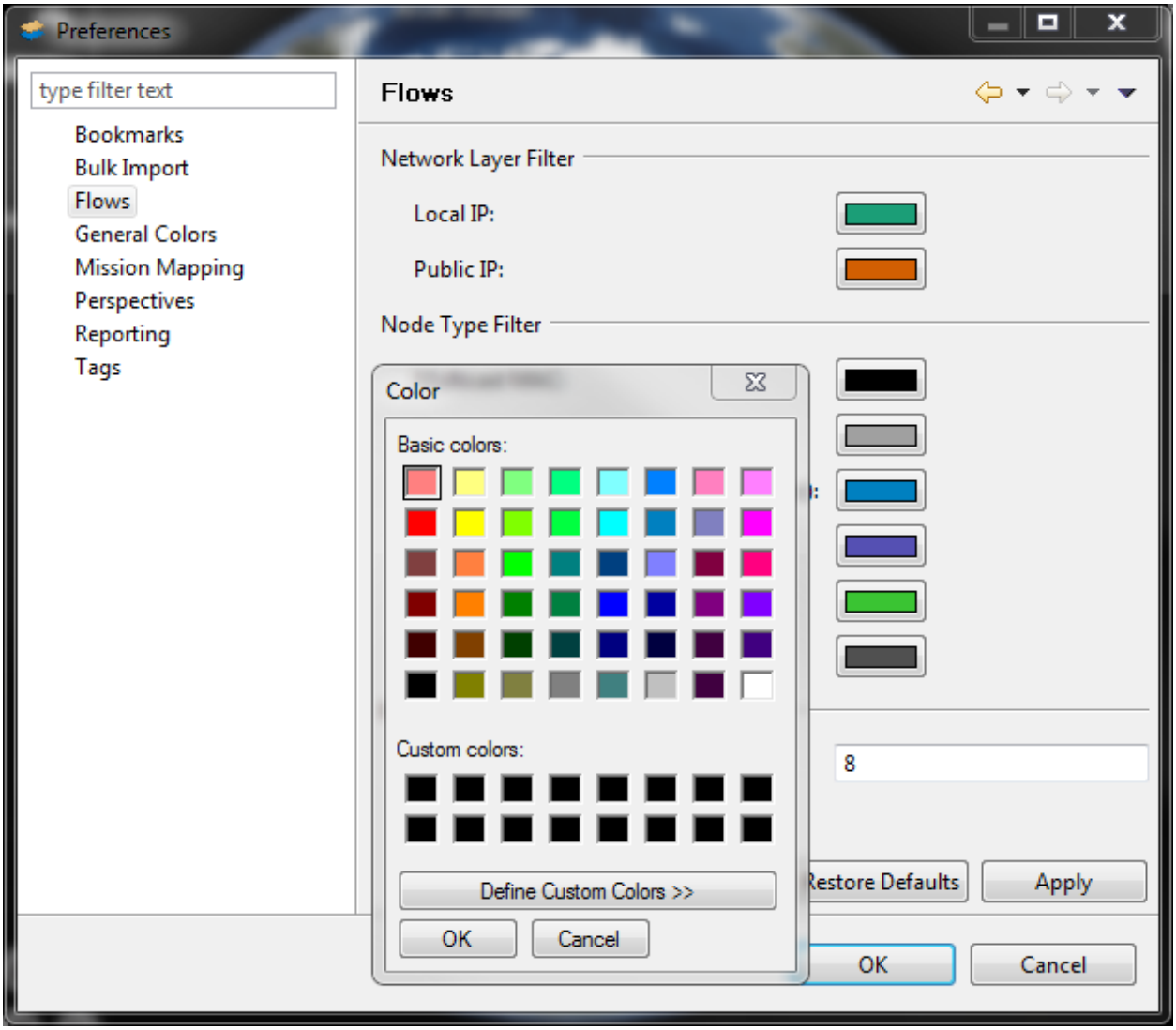


8.2 Flow Colors

The Flows View is capable of displaying many types of connections. To customize the display of connections in this View, from the MeerCAT main menu select **-> Window -> Preferences.** Then click on the **Flows** selection.



This page allows each address type – Broadcast MAC, Datalink MAC, Local IP, Remote IP, Wireless Network and Other – to have its own color. To change colors, click on the color to select from the color palette.

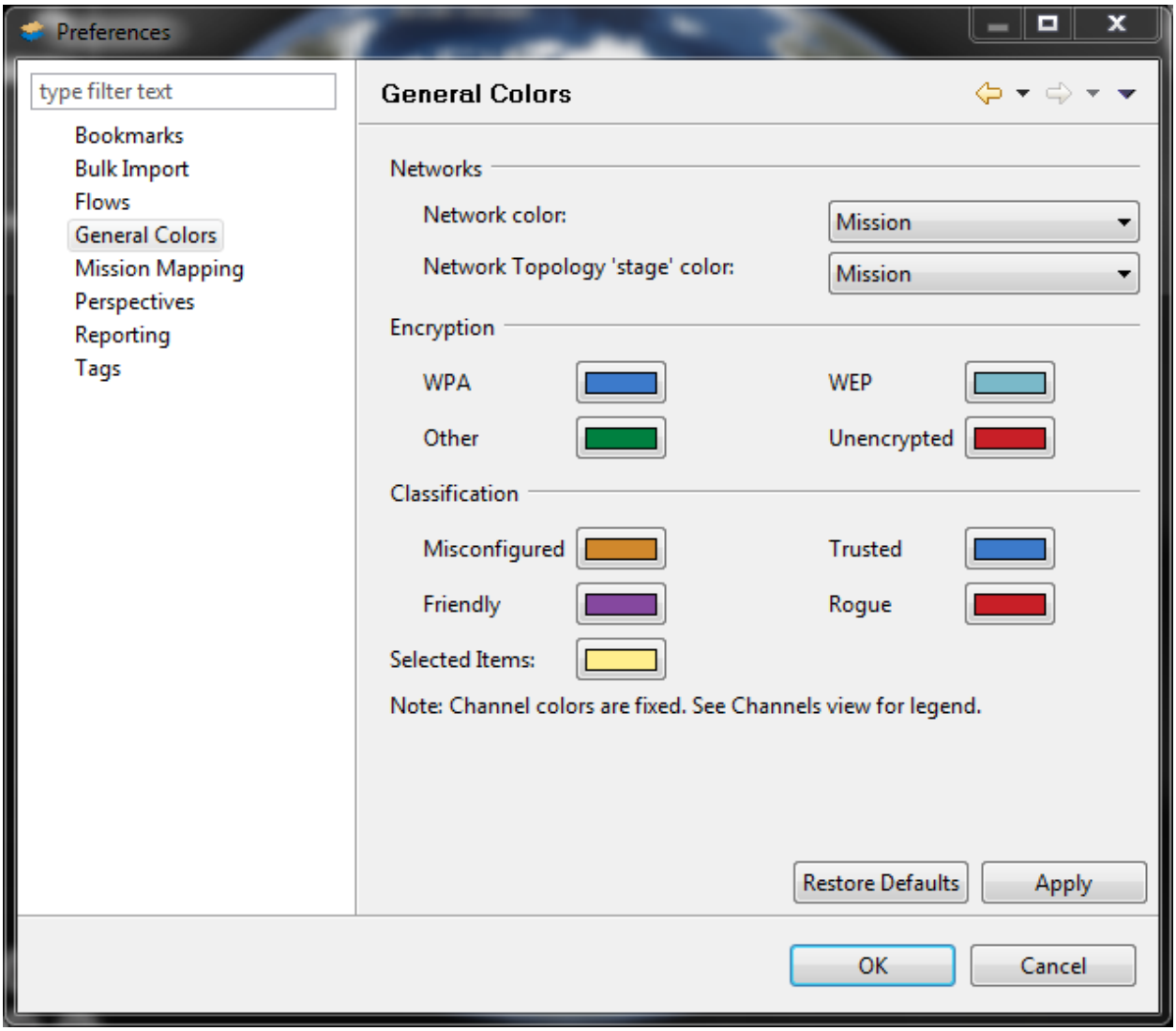


Colors used to depict the datalink layer vs. the network layer can also be customized.

Another feature of the Flows View which can be customized is the duration of the force-directed graphing feature of the display. The Flows View uses a technique which positions the nodes depicted in the View so that all the edges are of more or less equal length and which minimizes the crossing edges as much as possible. The number of seconds during which this technique is applied can be controlled by specifying the duration. As of this writing, the default is 8 seconds, seen in the screenshot above.

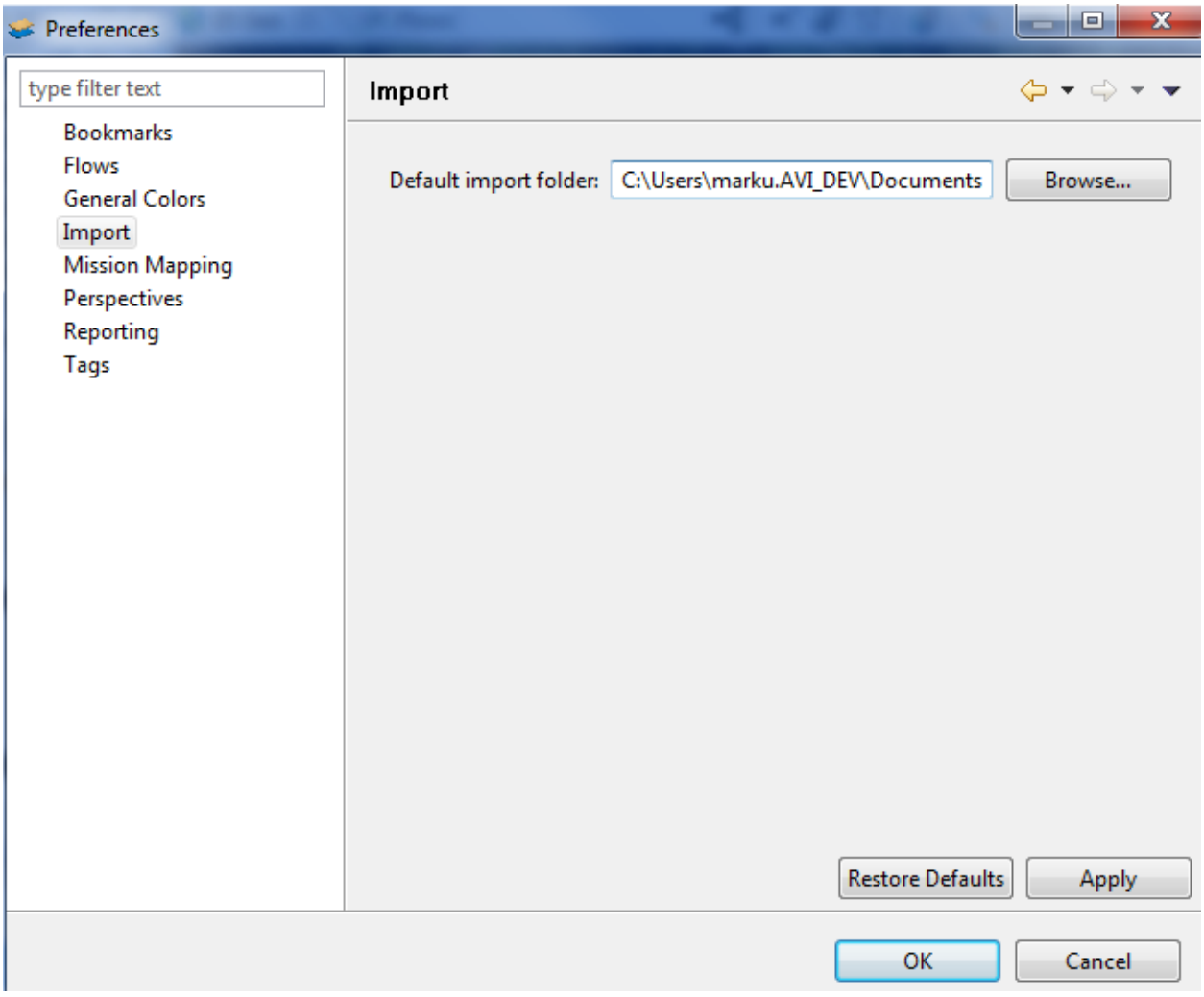
8.3 General Colors

Colors can be helpful in highlighting specific areas of interest throughout MeerCAT. To further manage color settings, it is possible to color wireless networks identified by MeerCAT according to Encryption, Channel, Classification or Mission. To perform such customization, select the **Window -> Preferences** submenu. Then choose **General Colors**. As shown below, select the type of coloring to be performed from the dropdown menu.



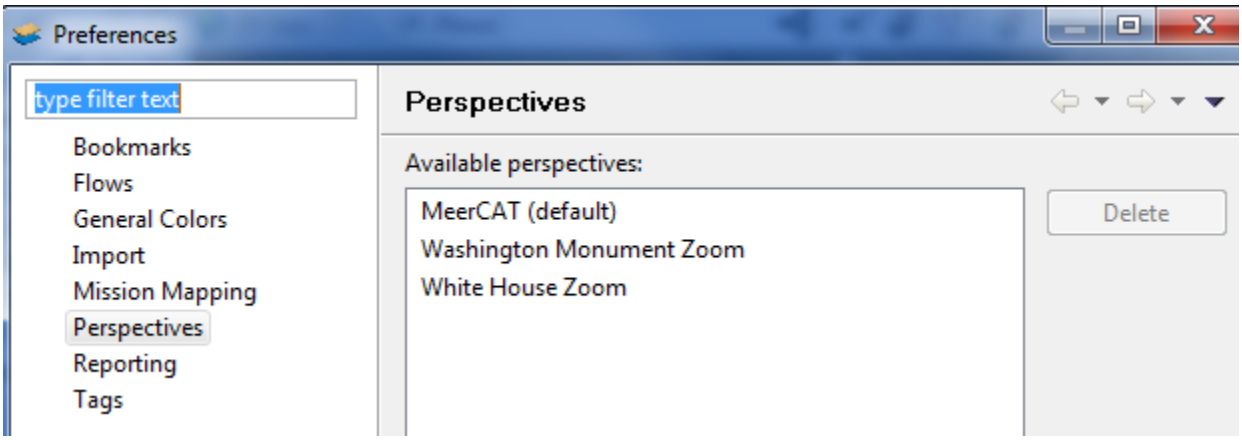
8.4 Import Folder

By default, MeerCAT looks for data to import in default user-specific folder, e.g., **c:\Users*username*.DOMAIN\Documents** (Windows 7). This can be changed by accessing the Import preference screen shown below.
Use the **Restore Defaults** button to switch back to the original MeerCAT default.



8.5 Maintain Perspectives

MeerCAT allows users to tailor different views to suit the particular style of analysis and type of task. Once these View settings – which views are showing, which options have been invoked, which zoom level is in effect, etc. -- have been created, they can be saved so that the workspace can be restored at any time. A list of available perspectives is available through the **Window -> Open Perspective** submenu. The same list is available through MeerCAT Preferences. Access the list through the **Window -> Preferences** and select **Perspectives** from the option list to the left.

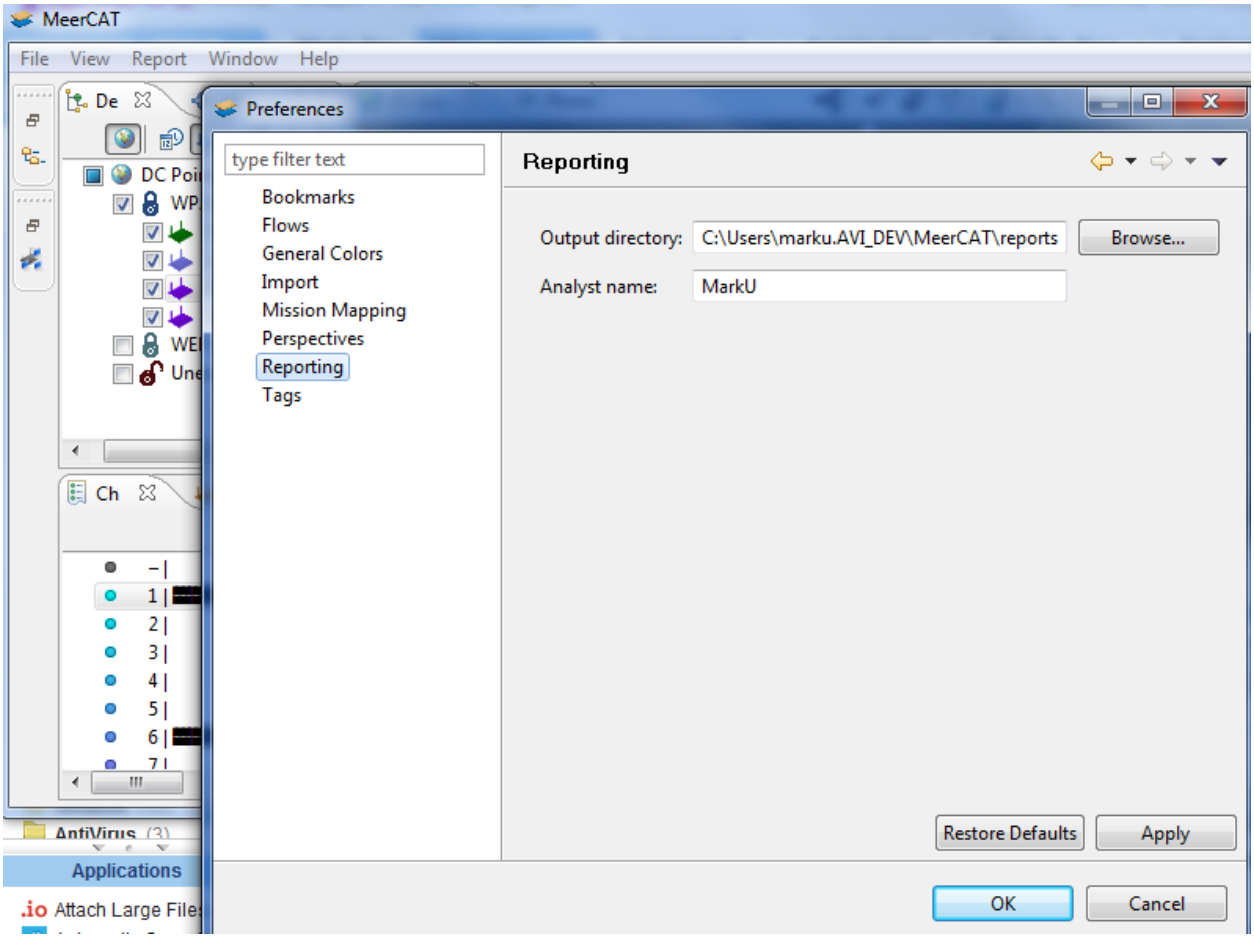


To remove a perspective, highlight it and click **Delete**.

8.6 Reporting Options

By default, reports created using MeerCAT are written to a default folder, e.g., **c:\Users\username.DOMAIN\MeerCAT**reports (Windows 7). A different folder can be specified by selecting Window -> Preferences from the main menu, and then selecting the **Reporting** option from the list on the left of the screen. This screen also permits the default analyst's name to be changed from the default.

Use the **Restore Defaults** button to return both values to the initial installation values.

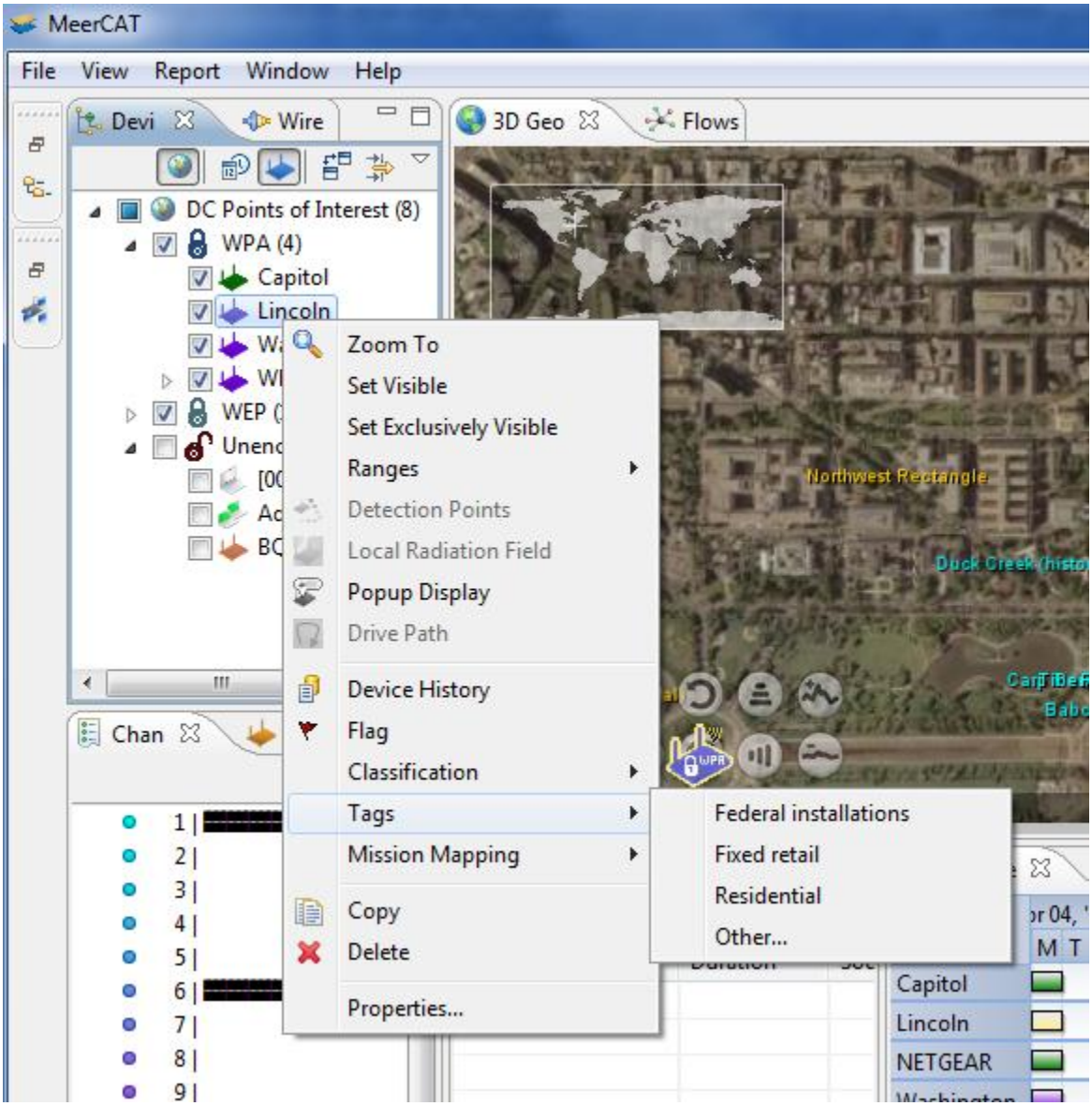


X

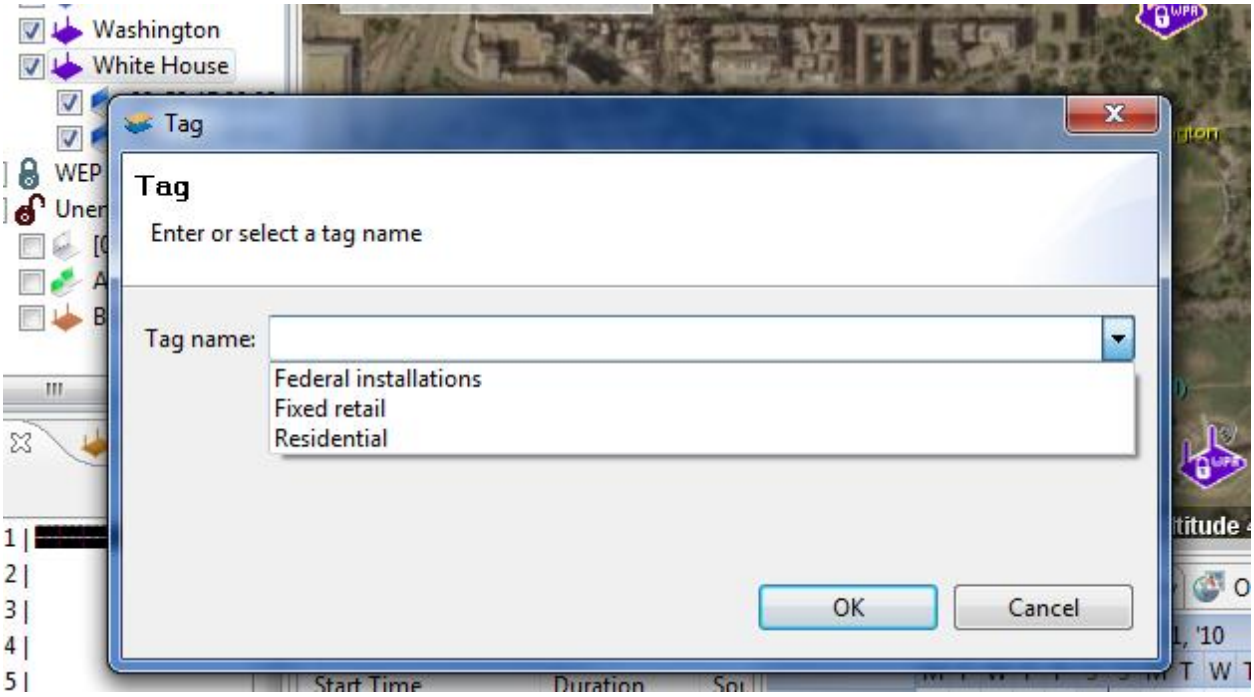
8.7 Tags

The Device Explorer View permits various features of networks and devices to be viewed in more detail. For instance, the Client Properties window allows the MAC address and Classification to be updated if necessary. The Wireless Network Properties window allows these, as well as additional fields, to be maintained. To aid in further grouping networks, wireless networks can be given short keywords, or tags.

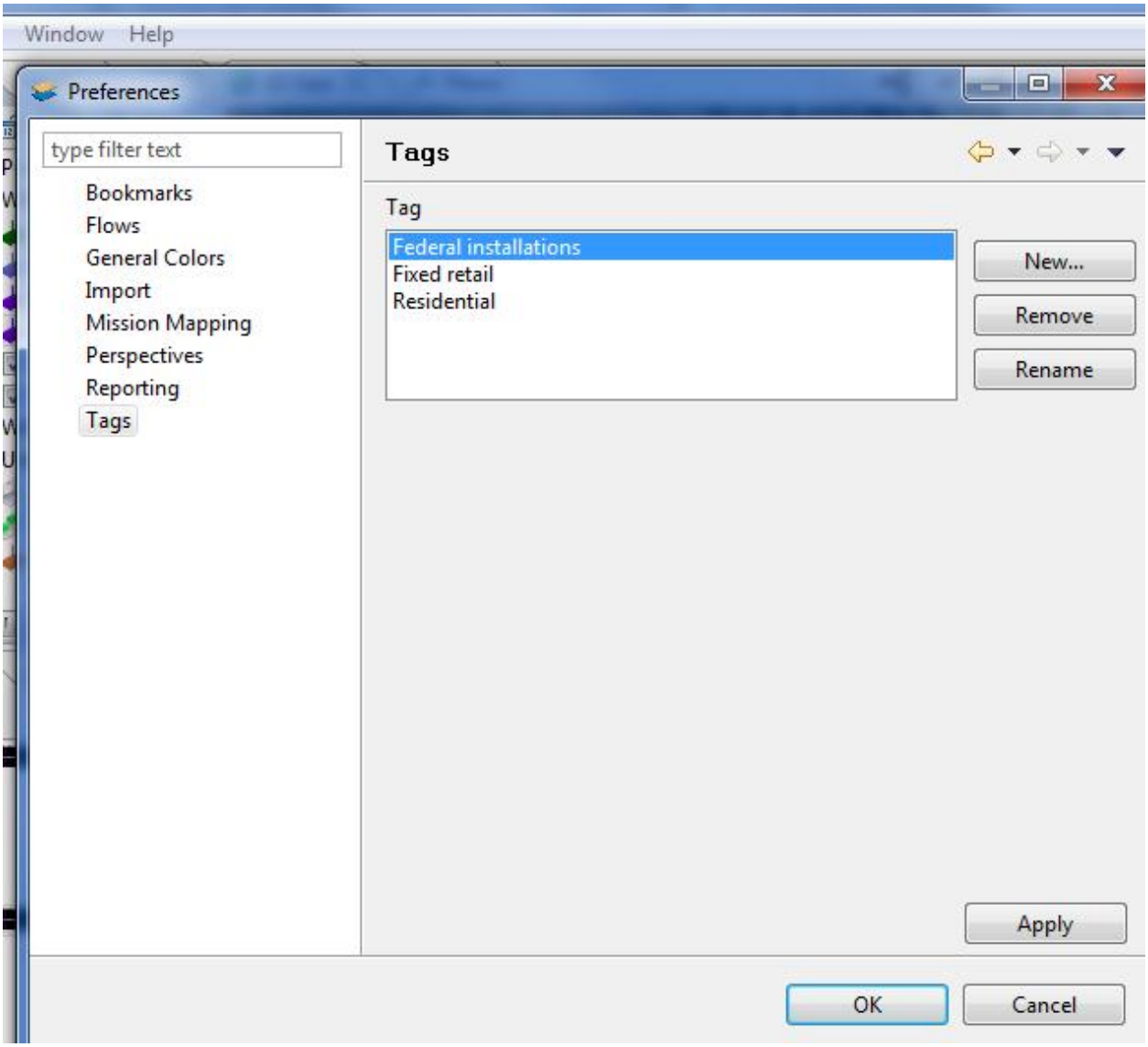
To assign a tag in the Device Explorer View, select a network and right-click. Select tag from the list of options. If tags have already been defined, these will be shown in the tag flyout menu, as shown below.



Existing tags can also be selected by choosing "**Other ...**" Use the following screen, which also allows new tags to be added as needed.



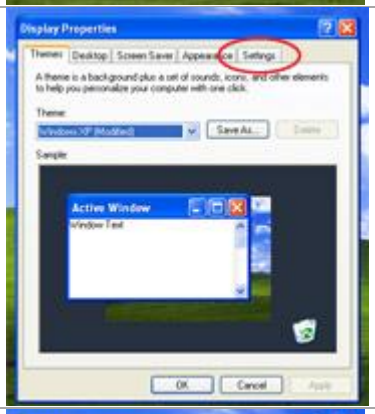
Once defined, tags can be maintained through the **Preferences** menu. Select the **Main Menu -> Window > Preferences** and then the **Tags** option from the list on the left. The window shown below allows tags to be added, deleted or renamed. Select **New...** to create a new tag. To remove or rename a tab, first highlight it, make changes as needed, then select **Rename** or **Remove**, as appropriate.



9 Frequently Asked Questions

1. The geographic globe appears but no imagery is displayed; only a halo outline.

This is commonly attributed to an outdated video card driver. Follow these steps to update your driver:

Step 1:	(These instructions are for Windows users.) On the desktop, right click and select "Properties".This will bring up the Display properties panel.	
Step 2:	At the top of the window, click on the "settings" tab. This will bring up detailed information for graphics and reveal the hardware vendor. This will be necessary to download the proper driver.	
Step 3:	In the middle of the screen is a pull-down menu labeled "Display". Read the contents of the box and look for one of three key words... **ATI**, **Nvidia**, or **Intel**.	
Step 4:	Download the appropriate driver based on the previous step. The drivers for each can be found at... **ATI / AMD** http://ati.amd.com/support/driver.html **Nvidia** http://www.nvidia.com/content/drivers/drivers.asp **Intel** http://www.intel.com/support/graphics/index.htm	
Step 5:	Download the driver to your desktop and run it, following all default instructions. This step may prompt your computer to reboot. Make certain any open applications have saved and allow the computer to reboot.	

If you still experience problems, this is sometimes related to the amount of memory allocated to MeerCAT. Decreasing the –JMX value as described in the next question sometimes resolves this issue.

You will also experience this behavior if running MeerCAT on a virtual machine or Remote Desktop Connection (RDC).

2. What is the best configuration for working with large datasets?

The MeerCAT.ini file located in your installation directory can be modified with a text editor to give MeerCAT more system memory. The –Xmx value represent the maximum amount of RAM given to MeerCAT. The default value is 768 MB. For systems will large amount of available memory, you may want to increase this value to 1024 MB or higher.

Another way to reduce memory requirements is to only have visible the views of interest. Closing views not in use will reduce memory load, especially views that have requested historical data.

Although you may notice memory usage peak, MeerCAT uses advanced caching and performance optimization to use available memory most efficiently.

3. How does MeerCAT determine a device's location?

If only the network XML file is imported, MeerCAT uses the center of the detection range (i.e., max+min lat / 2, max+min long / 2). If the GPS file is used then an average of the detected GPS points, weighted by the square of the signal strength is used, but only points whose signal strength is within 10% of the maximum (note that does not mean "top 10% of the points").